(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-46856
(P2004-46856A)
(43)公開日　平成16年2月12日(2004.2.12)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 12/14	G06F	12/14	310K	5B017
H04L 9/08	H04L	9/00	675B	5J104
H04L 9/32	H04L	9/00	675D	
	H04L	9/00	675Z	
	H04L	9/00	601E	

審査請求 未請求　請求項の数 28　OL　（全 41 頁）

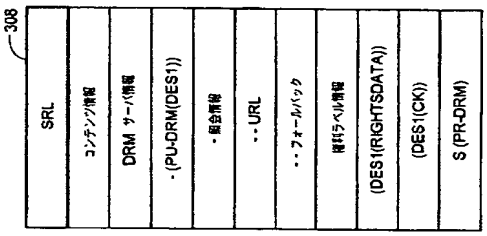
(21)出願番号　特願2003-183596(P2003-183596)
(22)出願日　平成15年6月26日(2003.6.26)
(31)優先権主張番号　10/185,527
(32)優先日　平成14年6月28日(2002.6.28)
(33)優先権主張国　米国(US)

(71)出願人　391055933
マイクロソフト　コーポレイション
ＭＩＣＲＯＳＯＦＴ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ　（番地なし）
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　スティーブン　ボーン
アメリカ合衆国　９８１２２　ワシントン州　シアトル　イースト　パイク　ストリート　３０３　ナンバー６０２

最終頁に続く

(54)【発明の名称】デジタルコンテンツに対応するデジタルライセンスを取得する方法

(57)【要約】
【課題】コンテンツは、コンテンツ鍵（ＣＫ）に従って暗号化され（ＣＫ（ｃｏｎｔｅｎｔ））、（ＣＫ）は、ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って保護され、コンテンツに関連する権利データは、（ＰＵ－ＤＲＭ）に従って保護される。
【解決手段】これら保護された項目は、ライセンスサーバによる署名を受けるために、権利ラベルとしてライセンスサーバに提出される。ライセンスサーバは、権利ラベルが有効か否かを検査し、有効であれば、保護された権利データに基づいてデジタル署名し、その結果として署名付き権利ラベル（ＳＲＬ）を得て、権利ラベルを戻す。ＳＲＬは、（ＣＫ（ｃｏｎｔｅｎｔ））と連結され、両方をユーザに配信する。コンテンツをレンダリングするために、ユーザは、ＳＲＬをライセンスサーバに提出してライセンスを要求する。
【選択図】　図５



【特許請求の範囲】
【請求項１】
デジタルコンテンツを公表し、ライセンスサーバが前記コンテンツに対応するライセンスを、前記コンテンツをレンダリングすることを望む１または複数のユーザに発行することを可能にする方法であって、
コンテンツ鍵（ＣＫ）に従って前記コンテンツを暗号化し、その結果として（ＣＫ（ｃｏｎｔｅｎｔ））を得ること、
前記ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って前記コンテンツ鍵（ＣＫ）を保護すること、
前記コンテンツに関連する権利データを生成すること、
（ＰＵ－ＤＲＭ）に従って前記権利データを保護すること、
前記保護された権利データと前記保護されたコンテンツ鍵（ＣＫ）とを権利ラベルとして、前記ライセンスサーバによる署名を受けるために、前記ライセンスサーバに提出し、前記ライセンスサーバは、前記権利ラベルが有効か否かを検査し、有効ならば、（ＰＵ－ＤＲＭ）に対応する秘密鍵（ＰＲ－ＤＲＭ）に基づいた、および少なくとも前記保護された権利データの一部に基づいたデジタル署名を生成し、その結果として署名付き権利ラベル（ＳＲＬ）を得て、該ＳＲＬを戻すこと、
前記戻されたＳＲＬを受け取り、前記受け取ったＳＲＬを（ＣＫ（ｃｏｎｔｅｎｔ））と連結してコンテンツパッケージを形成すること、および
前記コンテンツパッケージを前記１または複数のユーザに配信することにより、前記コンテンツをレンダリングすることを望むユーザは、前記コンテンツパッケージから前記ＳＲＬを取り出し、取り出されたＳＲＬを前記コンテンツに対応する前記ライセンスの要求の一部として前記ライセンスサーバに提出し、前記ライセンスサーバは、（ＰＵ－ＤＲＭ）に基づいて、および少なくとも前記保護された権利データの一部に基づいて前記ＳＲＬの署名を検査し、前記ＳＲＬ内の前記保護された権利データにアクセスし、該権利データをレビューして、前記ユーザがライセンスを受ける権利があるか否かを判断し、そうであれば、前記ユーザにライセンスを発行し、前記ライセンスは、ユーザにアクセス可能に保護された形で（ＣＫ）を含むこと
を備えたことを特徴とする方法。
【請求項２】
前記ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って前記コンテンツ鍵（ＣＫ）を保護することは、
対称鍵（ＤＥＳ１）を生成すること、
（ＤＥＳ１）に従って（ＣＫ）を暗号化し、その結果として（ＤＥＳ１（ＣＫ））を得ること、および
（ＰＵ－ＤＲＭ）に従って（ＤＥＳ１）を暗号化し、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得ることにより、前記ライセンスサーバは、（ＰＲ－ＤＲＭ）を使用して（ＣＫ）にアクセスすることができること
を備えたことを特徴とする請求項１に記載の方法。
【請求項３】
（ＤＥＳ１）に従って（ＣＫ）を暗号化し、その結果として（ＤＥＳ１（ＣＫ））を得た後に、（ＣＫ）を破棄することにより、（ＣＫ）を、（ＤＥＳ１（ＣＫ））を解読することによってのみ取得できることをさらに備えたことを特徴とする請求項２に記載の方法。
【請求項４】
（ＰＵ－ＤＲＭ）に従って前記権利データを保護することは、
対称鍵（ＤＥＳ１）を生成すること、
（ＤＥＳ１）に従って前記権利データを暗号化し、その結果として（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を得ること、および
（ＰＵ－ＤＲＭ）に従って（ＤＥＳ１）を暗号化し、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得ることにより、前記ライセンスサーバは、（ＰＲ－ＤＲＭ）を使用して（

ＣＫ）にアクセスすることができること
を備えたことを特徴とする請求項１に記載の方法。
【請求項５】
対称コンテンツ鍵（ＣＫ）に従って前記コンテンツを暗号化し、その結果として（ＣＫ（ｃｏｎｔｅｎｔ））を得ることを備えたことを特徴とする請求項１に記載の方法。
【請求項６】
前記コンテンツをレンダリングする権利を有する各エンティティと、各エンティティについて、前記エンティティが前記コンテンツをレンダリングすることに対して所持する各権利とを含む権利データを生成することを備え、各エンティティは、ユーザおよびユーザクラスの１つを備えたことを特徴とする請求項１に記載の方法。
【請求項７】
前記権利のうちの少なくとも一部の各々について、前記コンテンツをレンダリングすることに対して、前記権利を実施するための前提条件を有する前記エンティティを含む権利データを生成することを備えたことを特徴とする請求項６に記載の方法。
【請求項８】
前記保護された権利データ、前記保護されたコンテンツ鍵（ＣＫ）、および権利ラベルとしてそのＩＤを含んでいる前記コンテンツに関する情報を、前記ライセンスサーバによる署名を受けるために、前記ライセンスサーバに提出することを備えたことを特徴とする請求項１に記載の方法。
【請求項９】
前記ライセンスサーバは、前記ライセンスサーバの所在を見つけるためのアドレス情報を含む、前記ライセンスサーバ上の前記権利ラベル情報を追加し、前記サーバに関する情報を含むＳＲＬを戻し、前記方法は、前記サーバに関する情報を含む、前記戻されたＳＲＬを受け取ることを備えたことを特徴とする請求項１に記載の方法。
【請求項１０】
ライセンスサーバからユーザにデジタルライセンスを提供する方法であって、前記ライセンスは、ユーザが対応する公表されたデジタルコンテンツをレンダリングすることを可能にし、前記コンテンツは、コンテンツ鍵（ＣＫ）に従って暗号化され、その結果として（ＣＫ（ｃｏｎｔｅｎｔ））を得て、該（ＣＫ（ｃｏｎｔｅｎｔ））は、前記ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って保護された（ＣＫ）と、（ＰＵ－ＤＲＭ）に従って保護された権利データと、（ＰＵ－ＤＲＭ）に対応する秘密鍵（ＰＲ－ＤＲＭ）に基づいた、および少なくとも前記保護された権利データの一部に基づいたデジタル署名とを含む署名付き権利ラベル（ＳＲＬ）により付随して生じ、該方法は、
前記ＳＲＬとユーザ鍵とを、前記ユーザから前記ライセンスの要求の一部として受け取ること、
前記ＳＲＬ内の署名にアクセスすること、
（ＰＵ－ＤＲＭ）に基づいた、および少なくとも前記保護された権利データの一部に基づいた前記署名を検査すること、
前記ＳＲＬ内の前記保護された権利データにアクセスすること、
前記アクセスされた権利データをレビューして、ユーザが前記ライセンスを受ける権利があるか否かを判断すること、および
もしそうであれば、
前記ＳＲＬ内の前記保護された（ＣＫ）にアクセスし、
前記アクセスされた（ＣＫ）を前記受け取ったユーザ鍵に従って保護し、
前記ライセンスを前記ユーザに発行し、前記ライセンスは、前記ユーザ鍵に従って保護された（ＣＫ）を含み、これにより、前記ユーザは、前記ライセンスから（ＣＫ）にアクセスし、（ＣＫ）を（ＣＫ（ｃｏｎｔｅｎｔ））に適用し、その結果としてコンテンツが得られること
を備えたことを特徴とする方法。
【請求項１１】

ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って保護された（ＣＫ）は、対称鍵（ＤＥＳ１）に従って暗号化され、その結果として（ＤＥＳ１（ＣＫ））を得る（ＣＫ）と、（ＰＵ－ＤＲＭ）に従って暗号化され、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得る（ＤＥＳ１）とを備え、該方法は、
（ＰＲ－ＤＲＭ）を（ＰＵ－ＤＲＭ（ＤＥＳ１））に適用し、その結果として（ＤＥＳ１）を得ることと、
（ＤＥＳ１）を（ＤＥＳ１（ＣＫ））に適用し、その結果として（ＣＫ）を得ることとにより、
前記ＳＲＬ内の前記保護された（ＣＫ）にアクセスすること
を備えたことを特徴とする請求項１０に記載の方法。

【請求項１２】
（ＰＵ－ＤＲＭ）に従って保護された前記権利データは、対称鍵（ＤＥＳ１）に従って暗号化され、その結果として（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））を得る権利データと、（ＰＵ－ＤＲＭ）に従って暗号化され、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得る（ＤＥＳ１）とを備え、該方法は、
（ＰＲ－ＤＲＭ）を（ＰＵ－ＤＲＭ（ＤＥＳ１））に適用し、その結果として（ＤＥＳ１）を得ることと、
（ＤＥＳ１）を（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））に適用し、その結果として権利データを得ることとにより、
前記ＳＲＬ内の前記保護された権利データにアクセスすること
を備えたことを特徴とする請求項１０に記載の方法。

【請求項１３】
前記ＳＲＬおよびユーザの公開鍵（ＰＵ－ＵＳＥＲ）を、前記ユーザからの前記ライセンスの要求の一部として受け取ることを備え、前記ユーザが前記ライセンスを受ける権利がある場合には、前記アクセスされた（ＣＫ）を、前記受け取った（ＰＵ－ＵＳＥＲ）に従って暗号化し、その結果として（ＰＵ－ＵＳＥＲ（ＣＫ））を得て、（ＰＵ－ＵＳＥＲ（ＣＫ））を含む前記ライセンスを前記ユーザに発行し、これにより、前記ユーザは、（ＰＵ－ＵＳＥＲ）に対応する秘密鍵（ＰＲ－ＵＳＥＲ）を（ＰＵ－ＵＳＥＲ（ＣＫ））に適用し、その結果として（ＣＫ）を得ることにより、前記ライセンスから（ＣＫ）にアクセスすることができ、（ＣＫ）を（ＣＫ（ｃｏｎｔｅｎｔ））に適用し、その結果としてコンテンツを得ることを特徴とする請求項１０に記載の方法。

【請求項１４】
前記アクセスされた権利データは、前記コンテンツをレンダリングする権利を有する各エンティティと、各エンティティについて、前記エンティティが前記コンテンツをレンダリングすることに対して所持する各権利とを含み、前記方法は、前記アクセスされた権利データをレビューして、前記要求するユーザが前記コンテンツをレンダリングする権利を有するユーザであるか否かを判断することと、そうであれば、前記ライセンスを前記ユーザに発行することを備え、前記ライセンスは、前記コンテンツをレンダリングすることに対して、前記権利データに基づいて前記ユーザが有する各権利を含むことを特徴とする請求項１０に記載の方法。

【請求項１５】
前記アクセスされた権利データは、前記権利のうちの少なくとも一部の各々について、前記コンテンツをレンダリングすることに対して、前記権利を実施するための前提条件を有する前記エンティティを含み、前記方法は、前記要求するユーザが前記コンテンツをレンダリングする権利を有するユーザであれば、前記ライセンスを前記ユーザに発行することを備え、前記ライセンスは、前記コンテンツをレンダリングすることに対して、前記権利データに基づいて前記ユーザが有する各権利と、各々の権利について、前記権利データに基づいて権利を実施するための前提条件とを含むことを特徴とする請求項１４に記載の方法。

【請求項１６】

デジタルコンテンツと、該コンテンツに対応し、前記コンテンツをレンダリングするためにライセンスサーバによりユーザに発行されたデジタルライセンスとを組み合わせた方法であって、
前記コンテンツは、コンテンツ鍵（ＣＫ）に従って暗号化され、その結果として（ＣＫ（ｃｏｎｔｅｎｔ））を得て、該（ＣＫ（ｃｏｎｔｅｎｔ））は、対称鍵（ＤＥＳ１）に従って暗号化され、その結果として（ＤＥＳ１（ＣＫ））得る（ＣＫ）と、対称鍵（ＤＥＳ１）に従って暗号化され、その結果として（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））を得る権利データと、ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って暗号化され、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得る（ＤＥＳ１）と、（ＰＵ－ＤＲＭ）に対応する秘密鍵（ＰＲ－ＤＲＭ）に基づいた、および少なくとも（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））の一部に基づいたデジタル署名とを含む署名付き権利ラベル（ＳＲＬ）により付随して生じ、
前記ライセンスは、ユーザ鍵に従って保護された（ＣＫ）を含むことにより、前記ユーザは、前記ライセンスから（ＣＫ）にアクセスすることができ、（ＣＫ）を（ＣＫ（ｃｏｎｔｅｎｔ））に適用し、その結果として前記コンテンツを得て、前記ライセンスは、前記ユーザ鍵に従って暗号化された（ＤＥＳ１）をさらに含み、
前記ユーザが前記ＳＲＬ内の前記権利データを変更する方法は、
前記ユーザ鍵に従って暗号化された（ＤＥＳ１）を前記ライセンスから取り出すこと、
前記ユーザ鍵に従って暗号化された（ＤＥＳ１）を解読し、その結果として（ＤＥＳ１）を得ること、
（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））を前記ＳＲＬから取り出すこと、
（ＤＥＳ１）を（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））に適用し、その結果として前記権利データを得ること、
前記権利データを望み通りに変更すること、
変更された権利データを（ＤＥＳ１）に従って暗号化し、その結果として（ＤＥＳ１（ａｌｔｅｒｅｄｒｉｇｈｔＳｄａｔａ））を得ること、
（ＤＥＳ１（ａｌｔｅｒｅｄｒｉｇｈｔＳｄａｔａ））と（ＤＥＳ１（ＣＫ））を再公表権利ラベルとして、ライセンスサーバによる署名を受けるために、前記ライセンスサーバに提出し、前記ライセンスサーバは、前記再公表権利ラベルが有効か否かを検査し、有効ならば、（ＰＲ－ＤＲＭ）に基づいた、および少なくとも（ＤＥＳ１（ａｌｔｅｒｅｄｒｉｇｈｔＳｄａｔａ））の一部に基づいたデジタル署名を作成し、その結果として署名付き再公表権利ラベル（ＳＲＲＬ）を得て、該ＳＲＲＬを戻すこと、
前記戻されたＳＲＲＬを受け取り、前記受け取ったＳＲＲＬを（ＣＫ（ｃｏｎｔｅｎｔ））と連結してコンテンツパッケージを形成すること、および
前記コンテンツパッケージを前記１または複数のユーザに配信することにより、前記コンテンツをレンダリングすることを望むユーザは、前記コンテンツパッケージから前記ＳＲＲＬを取り出し、取り出したＳＲＲＬを前記コンテンツに対応する前記ライセンスの要求の一部として前記ライセンスサーバに提出し、前記ライセンスサーバは、（ＰＵ－ＤＲＭ）に基づいて、および少なくとも（ＤＥＳ１（ａｌｔｅｒｅｄｒｉｇｈｔＳｄａｔａ））の一部に基づいて前記ＳＲＲＬの署名を検査し、前記ＳＲＲＬ内の（ＤＥＳ１（ａｌｔｅｒｅｄｒｉｇｈｔＳｄａｔａ））にアクセスし、該（ＤＥＳ１（ａｌｔｅｒｅｄｒｉｇｈｔＳｄａｔａ））をレビューして、前記ユーザがライセンスを受ける権利があるか否かを判断し、そうであれば、前記ユーザにライセンスを発行し、前記ライセンスは、ユーザにアクセス可能な保護された形で（ＣＫ）を含むこと
を備えたことを特徴とする方法。
【請求項１７】
前記戻されたＳＲＲＬを受け取り、（ＣＫ（ｃｏｎｔｅｎｔ））から前記ＳＲＬを取り除き、前記受け取ったＳＲＲＬを（ＣＫ（ｃｏｎｔｅｎｔ））と連結してコンテンツパッケージを形成することを備えたことを特徴とする請求項１６に記載の方法。
【請求項１８】

前記ライセンスは、前記ユーザの公開鍵（ＰＵ－ＵＳＥＲ）に従って暗号化され、その結果として（ＰＵ－ＳＥＲ（ＣＫ））を得る（ＣＫ）、および（ＰＵ－ＵＳＥＲ）に従って暗号化され、その結果として（ＰＵ－ＵＳＥＲ（ＤＥＳ１））を得る（ＤＥＳ１）を含み、前記方法は、
（ＰＵ－ＵＳＥＲ（ＤＥＳ１））を前記ライセンスから取り出すこと、および
（ＰＵ－ＵＳＥＲ（ＤＥＳ１））を（ＰＵ－ＵＳＥＲ）に対応する前記ユーザの秘密鍵（ＰＲ－ＵＳＥＲ）に従って解読し、その結果として（ＤＥＳ１）を得ること
を含むことを特徴とする請求項１６に記載の方法。
【請求項１９】
デジタルコンテンツを自己公表し、ライセンスサーバが前記コンテンツに対応するライセンスを、前記コンテンツをレンダリングすることを望む１または複数のユーザに発行することを可能にする方法であって、
公開鍵（ＰＵ－ＣＥＲＴ）と、前記ユーザの公開鍵（ＰＵ－ＣＥＲＴ）に従って暗号化され、その結果として（ＰＵ－ＵＳＥＲ（ＰＲ－ＣＥＲＴ））を得る、対応する秘密鍵（ＰＲ－ＣＥＲＴ）とを含む許可証明書を前記ライセンスサーバから受け取り、前記許可証明書は、前記ライセンスサーバの秘密鍵（ＰＲ－ＤＲＭ）によって署名されていること、
前記コンテンツをコンテンツ鍵（ＣＫ）に従って暗号化し、その結果として（ＣＫ（ｃｏｎｔｅｎｔ））を得ること、
前記コンテンツ鍵（ＣＫ）を（ＰＲ－ＤＲＭ）に対応する前記ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って保護すること、
前記コンテンツに関連する権利データを生成すること、
権利データを（ＰＵ－ＤＲＭ）に従って保護すること、
前記保護された権利データと前記保護されたコンテンツ鍵（ＣＫ）とを権利ラベルとして提出すること、
前記受け取られた許可証明書から（ＰＲ－ＣＥＲＴ）を取得すること、
前記提出された権利ラベルを、少なくとも前記保護された権利データに基づいて取得された（ＰＲ－ＣＥＲＴ）で署名し、その結果として署名付き権利ラベル（ＳＲＬ）を得ること、
前記ＳＲＬおよび前記許可証明書と（ＣＫ（ｃｏｎｔｅｎｔ））とを連結してコンテンツパッケージを形成すること、および
前記コンテンツパッケージを前記１または複数のユーザに配信することにより、前記コンテンツをレンダリングすることを望むユーザは、前記コンテンツパッケージから前記ＳＲＬおよび前記許可証明書を取り出し、取り出されたＳＲＬおよび許可証明書を前記コンテンツに対応する前記ライセンスの要求の一部として前記ライセンスサーバに提出し、前記ライセンスサーバは、（ＰＵ－ＤＲＭ）に基づいて前記証明書の署名を検査し、前記証明書から（ＰＵ－ＣＥＲＴ）を取得し、取得された（ＰＵ－ＣＥＲＴ）に基づいたＳＲＬの署名を検査し、前記ＳＲＬ内の前記保護された権利データにアクセスし、該権利データをレビューして、前記ユーザがライセンスを受ける権利があるか否かを判断し、そうであれば、前記ユーザにライセンスを発行し、前記ライセンスは、ユーザにアクセス可能に保護された形で（ＣＫ）を含むこと
を備えたことを特徴とする方法。
【請求項２０】
前記受け取られた許可証明書から（ＰＲ－ＣＥＲＴ）を取得することは、前記証明書から（ＰＵ－ＵＳＥＲ（ＰＲ－ＣＥＲＴ））を取得し、（ＰＵ－ＵＳＥＲ）に対応するユーザの秘密鍵（ＰＲ－ＵＳＥＲ）を（ＰＵ－ＵＳＥＲ（ＰＲ－ＣＥＲＴ））し、その結果として（ＰＲ－ＣＥＲＴ）を得ることを備えたことを特徴とする請求項１９に記載の方法。
【請求項２１】
前記コンテンツ鍵（ＣＫ）を前記ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って保護することは、
対称鍵（ＤＥＳ１）を生成すること、

（ＣＫ）を（ＤＥＳ１）に従って暗号化し、その結果として（ＤＥＳ１（ＣＫ））を得ること、および
（ＤＥＳ１）を（ＰＵ－ＤＲＭ）に従って暗号化し、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得ることにより、前記ライセンスサーバは、（ＰＲ－ＤＲＭ）を使用して（ＣＫ）にアクセスすることができること
を備えたことを特徴とする請求項１９に記載の方法。
【請求項２２】
（ＤＥＳ１）に従って（ＣＫ）を暗号化し、その結果として（ＤＥＳ１（ＣＫ））を得た後に、（ＣＫ）を破棄することにより、（ＣＫ）を、（ＤＥＳ１（ＣＫ））を解読することによってのみ取得できることをさらに備えた特徴とする請求項２１に記載の方法。
【請求項２３】
（ＰＵ－ＤＲＭ）に従って前記権利データを保護することは、
対称鍵（ＤＥＳ１）を生成すること、
（ＤＥＳ１）に従って前記権利データを暗号化し、その結果として（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を得ること、および
（ＰＵ－ＤＲＭ）に従って（ＤＥＳ１）を暗号化し、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得ることにより、前記ライセンスサーバは、（ＰＲ－ＤＲＭ）を使用して（ＣＫ）にアクセスすることができること
を備えたことを特徴とする請求項１９に記載の方法。
【請求項２４】
対称コンテンツ鍵（ＣＫ）に従って前記コンテンツを暗号化し、その結果として（ＣＫ（ｃｏｎｔｅｎｔ））を得ることを備えたことを特徴とする請求項１９に記載の方法。
【請求項２５】
前記コンテンツをレンダリングする権利を有する各エンティティと、各エンティティについて、前記エンティティが前記コンテンツをレンダリングすることに対して所持する各権利とを含む権利データを生成することを備え、各エンティティは、ユーザおよびユーザクラスの１つを備えたことを特徴とする請求項１９に記載の方法。
【請求項２６】
前記権利のうちの少なくとも一部の各々について、前記コンテンツをレンダリングすることに対して、前記権利を実施するための前提条件を有する前記エンティティを含む権利データを生成することを備えたことを特徴とする請求項２５に記載の方法。
【請求項２７】
前記保護された権利データ、前記保護されたコンテンツ鍵（ＣＫ）、および権利ラベルとしてそのＩＤを含んでいる前記コンテンツに関する情報を、前記ライセンスサーバによる署名を受けるために、前記ライセンスサーバに提出することを備えたことを特徴とする請求項１９に記載の方法。
【請求項２８】
前記ライセンスサーバは、前記ライセンスサーバの所在を見つけるためのアドレス情報を含む、前記ライセンスサーバ上の前記権利ラベル情報を追加することを備えたことを特徴とする請求項１９に記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、デジタル権利管理（ＤＲＭ：ｄｉｇｉｔａｌ　ｒｉｇｈｔｓ　ｍａｎａｇｅｍｅｎｔ）システムに関する。より詳細には、本発明は、デジタルコンテンツの一部に対する署名付き権利ラベル（ＳＲＬ：Ｓｉｇｎｅｄ　ｒｉｇｈｔｓ　ｌａｂｅｌ）をライセンスサーバから取得する際に実行されるステップ、およびコンテンツに対応するデジタルライセンスをライセンスサーバから取得する際に実行されるステップに関する。
【０００２】
【従来の技術】

デジタル権利の管理と実施は、デジタルオーディオ、デジタルビデオ、デジタルテキスト、デジタルデータ、デジタルマルチメディアなどのデジタルコンテンツに関連して高く望まれている。ここで、このようなデジタルコンテンツは、1または複数のユーザに配信されている。デジタルコンテンツは、例えば、テキストドキュメントなど静的なものもあれば、ライブイベントのストリーム型オーディオ／ビデオなどストリーム化されているものもある。代表的な配信モードには、磁気（フロッピー（登録商標））ディスク、磁気テープ、光（コンパクト）ディスク（ＣＤ）などの有形デバイスと、電子掲示板、電子ネットワーク、インターネットなどの無形メディアとがある。デジタルコンテンツがユーザによって受信されると、ユーザは、パーソナルコンピュータ等のメディアプレーヤなどの、適当なレンダリングデバイスの助けを借りて、デジタルコンテンツをレンダリングし、または「プレイ」する。

【０００３】

あるシナリオでは、著者、出版者、放送者などの、コンテンツ所有者または権利所有者は、ライセンス料または他の何らかの対価と引き換えに、デジタルコンテンツを多数のユーザまたは受取人の各々に配信することを望んでいる。このようなシナリオでは、コンテンツは、歌曲、アルバム、映画などがあり、ライセンス料を生み出すことが配信の目的である。このようなコンテンツ所有者は、選択権が与えられていれば、ユーザが、このように配信されたデジタルコンテンツを扱うことに対して制限を設けたいと望むであろう。例えば、コンテンツ所有者は、少なくとも別のユーザからのライセンス料を受け取らないで、ユーザがコンテンツをコピーし、別のユーザに再配信するのを制限したい。

【０００４】

さらに、コンテンツ所有者は、ユーザに異なる種類の使用ライセンスを異なるライセンス料で購入する柔軟性を与えると同時に、ユーザを実際に購入されたどの種類のライセンスの条項で拘束するかの柔軟性を与えることを望む場合がある。例えば、コンテンツ所有者は、配信されたデジタルコンテンツを、制限された回数だけ、ある時間だけ、ある装置の種類だけ、あるメディアプレーヤの種類だけ、あるユーザの種類だけプレイできるようにすることを望む場合がある。

【０００５】

別のシナリオでは、企業内の従業員などのコンテンツ開発者は、そのデジタルコンテンツを、企業内の1または複数の他の従業員または企業外の他の個人に配信することを望むが、他人にコンテンツをレンダリングさせないことを望む場合がある。ここでは、コンテンツの配信は、ラインセンス料または他の何らかの対価と引き換えに広く配信するのとは異なり、企業におけるコンテンツを機密または制限された形で共有するのと似ている。このシナリオでは、コンテンツは、ドキュメントプレゼンテーション、スプレッドシート、データベース、電子メールなどであり、オフィス施設内でやりとりされる。コンテンツ開発者は、コンテンツがオフィス施設内に留まっていて、例えば、競業者または敵対者などの無許可の個人によりレンダリングされないことが保障されることを望む場合がある。このとき、そのコンテンツ開発者は、配信されたデジタルコンテンツを受取人がどのように扱うかについて制限を設けることを望んでいる。例えば、コンテンツ所有者は、少なくともコンテンツをレンダリングすることを許されている個人の範囲外にコンテンツが公開される方法で、ユーザがそのコンテンツをコピーし、別のユーザに再配信するのを制限したいと望んでいる。

【０００６】

さらに、コンテンツ開発者は、異なるレベルでレンダリングする権利を、種々の受取人に与えたいと望む場合がある。例えば、コンテンツ開発者は、保護されたデジタルコンテンツを、あるクラスの個人に対しては表示可能・印刷不能にし、別のクラスの個人に対しては表示可能・印刷可能にすると望む場合がある。

【０００７】

しかし、どちらのシナリオの場合も、配信が行われた後は、そのコンテンツ所有者／開発者は、デジタルコンテンツに対して制御できたとしても、その制御は無に等しい。このこ

とが特に問題となっているのは、ほとんどのパーソナルコンピュータも、デジタルコンテンツをそのままデジタルコピーし、そのデジタルコピーを、書き込み可能な磁気または光ディスクにダウンロードし、またはそのデジタルコピーを、インターネットなどのネットワーク経由で別のデスティネーションへ送信するのに必要なソフトウェアとハードウェアとを備えているからである。

【０００８】

当然のことであるが、コンテンツが配信されるトランザクションの一部として、コンテンツ所有者／開発者は、デジタルコンテンツのユーザ／受取人に要求して、そのデジタルコンテンツを望ましくない方法で再配信しないとの約束をすることができる。しかし、このような約束は容易に行われ、容易に破られる。コンテンツ所有者／開発者は、いくつかの公知のセキュリティデバイスのいずれかを通して、このような再配信を禁止することを試みることができ、通常は、暗号化と暗号解読が伴う。しかし、優柔不断なユーザ（ｍｉｌｄｌｙ ｄｅｔｅｒｍｉｎｅｄ ｕｓｅｒ）が暗号化デジタルコンテンツを解読し、そのデジタルコンテンツを非暗号化形式でセーブした後、その再配信を防止できる見込みはほとんどない。

【０００９】

【発明が解決しようとする課題】

任意形態のデジタルコンテンツの制御されたレンダリングまたはプレイを行うことを可能にするデジタル権利管理、実施アーキテクチャ及びその方法を提供することが要望され、その制御は、フレキシブルで、そのデジタルコンテンツのコンテンツ所有者／開発者によって定義可能である。より具体的には、特にオフィス、組織環境、またはドキュメントが特定の個人グループまたは特定の個人クラスの間で共有されるような、制御されたレンダリングを行うことを可能にし、容易にするアーキテクチャが要望されている。

【００１０】

【課題を解決するための手段】

本発明は、デジタルコンテンツとサービスの使用ライセンスを、署名付き権利ラベル（ＳＲＬ）を介して、発行するシステムと方法を提供することによって、「従来の技術」の個所で上述した要求を解決している。

【００１１】

本発明によれば、デジタル権利管理（ＤＲＭ）ライセンス発行コンポーネントは、別のソフトウェアアプリケーションまたはコンポーネントが、ライセンスによって規定された条項に従ってデジタルコンテンツまたはサービスを消費するのを可能にするライセンスを発行する。ライセンスを発行するために、ライセンス発行コンポーネントは、一組の条項を規定している権利ラベルを使用し、その条項から１つの特定ライセンスを発行することを可能にしている。ライセンス条項は、コンテンツまたはサービスを使用する権利、条件、および本人を規定している。ここで用いられている「権利」という用語は、消費側コンポーネントによって理解される特定の動作である（例えば、デジタルメディアプレーヤでは「プレイ」、ドキュメント管理システムでは「編集」）。ここで用いられている「条件」という用語は、消費側コンポーネントがその消費を行うのを許可する前に満たされていなければならない特定の基準である（例えば、「１２月１日より遅くない」）。さらに、ライセンスには、ライセンスの対象となっている、保護されたコンテンツまたはサービスのロックを解除するために使用される暗号化鍵マテリアルを含むこともできる。本発明による権利ラベルは、その権利ラベルが関連付けられているコンテンツまたはサービスに対して許可可能に発行される、すべてのライセンスの境界を定める定義を含む。従って、一般的に、ライセンスは、権利ラベルの中で規定された権利と条件のサブセットを含む。

【００１２】

本発明は、コンテンツの一部に対する権利記述および関連する保護された暗号化鍵マテリアルを受信すること、権利ラベルを生成するためにこのデータに対するデジタル署名の有効性を検査して生成すること、アプリケーションがコンテンツの一部に対するライセンスを要求するのを可能にすること、ＤＲＭライセンシングサーバが上記要求に対する許可検

査を行うのを可能にすること、ＤＲＭライセンシングサーバが要求に基づいて要求側にライセンスを発行し、要求を行うアプリケーションまたはユーザに対するコンテンツの暗号化マテリアルを保護するのを可能にすることを含む機能を実行するプロトコルおよび／またはアプリケーションプログラムおよび／またはアプリケーションプログラムインタフェース（ＡＰＩ）として実現することができる。

【００１３】

本発明の一実施形態では、デジタルコンテンツは、コンテンツをレンダリングすることを望んでいる１または複数のユーザに対応するデジタルライセンスを、ライセンスサーバが発行するのを可能にするために公表される。コンテンツは、コンテンツ鍵（ＣＫ）によって暗号化され、その結果として（ＣＫ（ｃｏｎｔｅｎｔ））が得られ、コンテンツ鍵（ＣＫ）は、ライセンスサーバの公開鍵（ＰＵ－ＤＲＭ）に従って保護され、コンテンツに関連する権利データは、（ＰＵ－ＤＲＭ）に従って生成され、保護される。

【００１４】

保護された権利データと保護されたコンテンツ鍵（ＣＫ）は、ライセンスサーバによる署名を受けるために権利ラベルとしてライセンスサーバに提出される。

ライセンスサーバは、権利ラベルの有効性を検査し、有効であれば、ＰＵ－ＤＲＭに対応する秘密鍵（ＰＲ－ＤＲＭ）に基づいて、少なくともその一部が保護された権利データに基づいたデジタル署名を生成し、その結果として署名付き権利ラベル（ＳＲＬ）が得られ、そのＳＲＬが戻される。

【００１５】

戻されたＳＲＬが受信されると、（ＣＫ（ｃｏｎｔｅｎｔ））と連結されてコンテンツパッケージが形成され、このコンテンツパッケージは、１または複数のユーザに配信される。コンテンツをレンダリングすることを望むユーザは、コンテンツパッケージからＳＲＬを取り出し、取り出したＳＲＬをコンテンツに対応するライセンス要求の一部としてライセンスサーバに提出する。ライセンスサーバは、ＰＵ－ＤＲＭに基づいて、少なくともその一部が保護された権利データに基づいたＳＲＬの署名を検査し、ＳＲＬ内の保護された権利データにアクセスし、アクセスした権利データをレビューして、ユーザがライセンスを受ける権利があるか否かを判断し、権利があれば、ライセンスをユーザに発行する。ライセンスは、ユーザにアクセス可能な保護された形式で、ＣＫを含んでいる。

【００１６】

【発明の実施の形態】

本発明のその他の特徴は、添付図面を参照して以下に詳述する本発明の実施形態の説明の中で明らかにする。

【００１７】

（例示コンピューティングデバイス）

図１と以下の説明は、本発明を実現するのに適しているコンピューティング環境の概要を要約して説明することを目的としている。なお、当然に理解されるように、ハンドヘルド、ポータブル、およびあらゆる種類の他のコンピューティングデバイスが本発明に関連して使用されることが意図されている。以下では汎用コンピュータが説明されているが、これは単なる一例にすぎず、本発明が必要としているのは、ネットワークサーバが相互に動作可能で、対話可能なシンクライアント（ｔｈｉｎ　ｃｌｉｅｎｔ）だけである。従って、本発明を、クライアントリソースの実装をほとんど必要としないか、または最小限で済むようなネットワーク化されたホスト中心のサービスの環境、例えば、クライアントデバイスがワールドワイドウェブの単なるブラウザまたはインタフェースとして働くネットワーク化された環境で実現することができる。

【００１８】

必ずしもその必要はないが、本発明を、開発者によって使用されるようにアプリケーションプログラミングインタフェース（ＡＰＩ）で実現することも、および／またはプログラムモジュールのように、クライアントワークステーション、サーバ、またはその他のデバイスなど１または複数のコンピュータによって実行されるコンピュータ実行可能命令とい

う広い文脈の中で、以下に説明されているネットワークブラウジングソフトウェアに含むこともできる。一般的に、プログラムモジュールは、特定のタスクを実行し、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。典型的には、プログラムモジュールの機能を、種々の実施形態での要求に応じて組み合わせたり、分散させたりすることができる。さらに、この当業者ならば理解されるように、本発明は、他のコンピュータシステム構成で実施することができる。本発明で使用するのに適している、他の周知コンピューティングシステム、環境および／または構成としては、これらに限定されないが、パーソナルコンピュータ（ＰＣ）、自動預金支払機、サーバコンピュータ、ハンドヘルドまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、プログラマム可能な家庭電化製品、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータなどがある。本発明は、タスクが通信ネットワークや他のデータ伝送媒体を通してリンクされているリモート処理デバイスによって実行されるような、分散型コンピューティング環境で実施することもできる。分散型コンピューティング環境では、プログラムモジュールを、メモリ記憶装置を含む、ローカルとリモートの両方のコンピュータ記憶媒体に配置することができる。

【００１９】

図１は、本発明を実現することができる適当なコンピューティングシステム環境１００の例を示しているが、上記説明から明らかであるように、このコンピューティングシステム環境１００は、適当なコンピューティング環境の単なる一例であり、本発明の使用または機能範囲を限定することを示唆するものではない。

また、このコンピューティング環境１００は、例示動作環境１００に示されているコンポーネントのいずれか１つ、またはどのような組み合わせに関しても、依存関係や要求条件があることを意味するものでもない。

【００２０】

図１を参照して説明すると、本発明を実現するための例示システムは、コンピュータ１１０の形態をした汎用コンピューティングデバイスを含む。コンピュータ１１０のコンポーネントは、これらに限定されないが、処理ユニット１２０、システムメモリ１３０、およびシステムメモリを含む種々のシステムコンポーネントを処理ユニット１２０に結合しているシステムバス１２１がある。システムバス１２１は、数種類のバス構造のいずれかにすることができ、このようなバス構造としては、メモリバスやメモリコントローラ、ペリフェラルバス、および種々のバスアーキテクチャのいずれかを採用しているローカルバスがある。例を挙げると、このようなアーキテクチャは、これらに限定されないが、ＩＳＡ（Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＭＣＡ（Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＥＩＳＡ（Ｅｎｈａｎｃｅｄ ＩＳＡ）バス、ＶＥＳＡ（Ｖｉｄｅｏ ＥｌｅｃｔｒｏｎｉｃＳ Ｓｔａｎｄａｒｄｓ ＡＳＳｏｃｉａｔｉｏｎ）ローカルバス、およびＰＣＩ（ＰｅｒｉＰｈｅｒａｌ ＣｏｍＰｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ）バス（Ｍｅｚｚａｎｉｎｅバスとも呼ばれている）がある。

【００２１】

コンピュータ１１０は、典型的には、種々のコンピュータ読取り可能媒体を装備しているのが代表的である。コンピュータ読取り可能媒体は、コンピュータ１１０によってアクセスできる媒体として利用可能なものであれば、どのような媒体にすることもでき、揮発性媒体と不揮発性媒体で、取り外し可能と取り外し不能の媒体が含まれている。例を挙げると、コンピュータ読取り可能媒体は、これらに限定されないが、コンピュータ記憶媒体と通信媒体がある。コンピュータ読取り可能媒体は、コンピュータ読取り可能命令、データ構造、プログラムモジュールまたは他のデータなどの、情報を格納するための方法または技術で実現された揮発性及び不揮発性、取り外し可能及び取り外し不能の媒体を含む。コンピュータ記憶媒体は、これらに限定されないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリや他のメモリ技術、ＣＤＲＯＭ、ＤＶＤ（ｄｉｇｉｔａｌ ｖｅｒｓａｔｉ

ｌｅ ｄｉｓｋ）または他の光ディスクストレージ、磁気カセット、磁気テープ、磁気ディスクストレージや他の磁気記憶装置、または必要とする情報を格納するために使用することができ、コンピュータ１１０によってアクセス可能である他の媒体などを含む。通信媒体は、典型的には、コンピュータ読取り可能命令、データ構造、プログラムモジュールまたは他のデータを、搬送波や他の伝送機構などの変調されたデータ信号の形で具現化し、任意の情報配達媒体が含まれている。ここで「変調されたデータ信号」という用語は、信号中の情報を符号化するような方法で１または複数の特性が設定または変更されている信号を意味している。例を挙げると、通信媒体は、これらに限定されないが、ワイヤドネットワークまたはダイレクトワイヤド接続などのワイヤド媒体、および音響、ＲＦ、赤外線、および他のワイレス媒体などのワイヤレス媒体を含む。上述のどのような組み合わせも、コンピュータ読取り可能媒体の範囲に含まれる。

【００２２】

システムメモリ１３０は、ＲＯＭ（ｒｅａｄ ｏｎｌｙ ｍｅｍｏｒｙ）１３１、ＲＡＭ（ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ）１３２などのように、揮発性および／または不揮発性メモリの形体をしたコンピュータ記憶媒体を含む。スタートアップ時など、コンピュータ１１０内の要素間で情報を転送するのを支援する基本ルーチンから構成されたＢＩＯＳ（ｂａｓｉｃ ｉｎＰｕｔ／ｏｕｔＰｕｔ ｓｙＳｔｅｍ）１３３は、典型的には、ＲＯＭ１３１に格納されている。ＲＡＭ１３２は、典型的には、即時に処理ユニット１２０によりアクセスされ、および／または処理されるデータおよび／またはプログラムモジュールを含む。例を挙げると、これらに限定されないが、図１は、オペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７を示す。

【００２３】

コンピュータ１１０は、他の取り外し可能／取り外し不能、揮発性／不揮発性のコンピュータ記憶媒体を装備することもできる。単なる例示として、図１は、取り外し不能で不揮発性の磁気媒体との間で読み書きを行うハードディスクドライブ１４１、取り外し可能で不揮発性の磁気ディスク１５２との間で読み書きを行う磁気ディスクドライブ１５１、およびＣＤＲＯＭや他の光媒体などの、取り外し可能で不揮発性の光ディスク１５６との間で読み書きを行う光ディスクドライブ１５５を示す。例示動作環境で使用できる、他の取り外し可能／取り外し不能、揮発性／不揮発性のコンピュータ記憶媒体は、これらに限定されないが、磁気テープカセット、フラッシュメモリカード、ＤＶＤ、デジタルビデオテープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭなどを含む。ハードディスクドライブ１４１は、典型的には、インタフェース１４０のような取り外し不能メモリインタフェースを介して、システムバス１２１に接続されている。磁気ディスクドライブ１５１と光ディスクドライブ１５５は、インタフェース１５０のような取り外し可能メモリインタフェースによりシステムメモリ１２１に接続されている。

【００２４】

上述した、図１に図示されたドライブとそれに関連するコンピュータ記憶媒体は、コンピュータ読取り可能命令、データ構造、プログラムモジュールおよび他のデータをコンピュータ１１０のために格納している。図１には、例えば、ハードディスクドライブ１４１は、オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラム１４７を格納しているものとして示されている。なお、これらのコンポーネントは、オペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７と同じであることもあれば、異なっていることもある。オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラムデータ１４７が異なる番号になっているのは、これらが、最低限、異なるコピーであることを示すためである。ユーザは、キーボード１６２およびマウス、トラックボールまたはタッチパッドとも広く呼ばれているポインティングデバイス１６１などの入力デバイスを通して、命令と情報とをコンピュータ１１０に入力することができる。その他の入力デ

バイス（図示せず）は、マイクロホン、ジョイスティック、ゲームパッド、衛星アンテナ、スキャナなどを含む。これらおよび他の入力デバイスは、システムバス１２１に結合されているユーザ入力インタフェース１６０を通して、処理ユニット１２０に接続されているが、パラレルポート、ゲームポートまたはＵＳＢ（ｕｎｉｖｅｒｓａｌ ｓｅｒｉａｌ ｂｕｓ）などの他のインタフェースやバス構造で接続されていることもある。

【００２５】

モニタ１９１、他の種類の表示装置は、ビデオインタフェース１９０のようなインタフェースを介して、システムバス１２１に接続されている。Ｎｏｒｔｈｂｒｉｄｇｅなどのグラフィックスインタフェース１８２を、システムバス１２１に接続することができる。Ｎｏｒｔｈｂｒｉｄｇｅは、ＣＰＵ、またはホストの処理ユニット１２０と通信し、ＡＧＰ（ａｃｃｅｌｅｒａｔｅｄ ｇｒａＰｈｉｃｓ Ｐｏｒｔ）との通信を担当するチップセットである。１または複数のグラフィックス処理ユニット（ＧＰＵ：ｇｒａＰｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ）１８４は、グラフィックスインタフェース１８２と通信することができる。この点に関して、ＧＰＵ１８４は、一般的に、レジスタストレージのような、オンチップメモリストレージを含み、ＧＰＵ１８４は、ビデオメモリ１８６とやりとりしている。なお、ＧＰＵ１８４は、コプロセッサの単なる一例であり、種々のコプロセッサデバイスをコンピュータ１１０に含めることができる。モニタ１９１または他のタイプディスプレイデバイスは、ビデオインタフェース１９０のような、インタフェースを介してシステムバス１２１に接続され、インタフェースは、ビデオメモリ１８６と通信することができる。モニタ１９１のほかに、スピーカ１９７、プリンタ１９６などの、他の周辺出力装置をコンピュータに含むこともでき、これらの出力デバイスを、出力周辺インタフェース１９５を通して接続することができる。

【００２６】

コンピュータ１１０は、リモートコンピュータ１８０などの、１または複数のリモートコンピュータとの論理的コネクションを使用するネットワーク化された環境で動作することができる。リモートコンピュータ１８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイスまたは他の共通ネットワークノードにすることができ、図１にはメモリ記憶装置１８１だけが示されているが、典型的には、コンピュータ１１０に関して上述した要素の多くまたはすべてを含む。図１に示した論理的コネクションは、ＬＡＮ（ｌｏｃａｌ ａｒｅａ ｎｅｔｗｏｒｋ）１７１とＷＡＮ（ｗｉｄｅ ａｒｅａ ｎｅｔｗｏｒｋ）１７３とがあるが、他のネットワークを含めることもできる。このようなネットワーキング環境は、オフィス、企業内コンピュータネットワーク、イントラネットおよびインターネットとして普通になっている。

【００２７】

ＬＡＮネットワーキング環境で使用されるときに、コンピュータ１１０は、ネットワークインタフェースまたはアダプタ１７０を通してＬＡＮ１７１に接続されている。ＷＡＮネットワーキング環境で使用されるときに、コンピュータ１１０は、典型的には、インターネットなどのＷＡＮ１７３上の通信を確立するためのモデム１７２または他の手段を含む。モデム１７２は、内蔵型と外付け型があり、どちらも、ユーザ入力インタフェース１６０または他の適当な機構を介してシステムバス１２１に接続することができる。ネットワーキング環境では、コンピュータ１１０に関して上述したプログラムモジュールまたはその一部は、リモートのメモリ記憶装置に格納しておくことができる。図１は、単なる一例であり、これに限定されないが、リモートのアプリケーションプログラム１８５は、メモリデバイス１８１に置かれているものとして示されている。当然に理解されるように、図示のネットワークコネクションは単なる例であり、コンピュータ間の通信リンクを確立する他の手段を使用することもできる。

【００２８】

当業者ならば理解されるように、コンピュータ１１０または他のクライアントデバイスは、コンピュータネットワークの一部として配置することができる。この点に関して、本発明は、任意の数のメモリまたは記憶ユニットを有し、任意の数のアプリケーションとプロ

セスとが任意の数の記憶ユニットまたはボリュームにわたって実行されている、あらゆるコンピュータシステムにも関係する。本発明は、サーバコンピュータとクライアントコンピュータがネットワーク環境内に配置され、リモートまたはローカルのストレージを有している環境に適用することができる。本発明は、プログラミング言語機能、翻訳機能および実行機能を備えたスタンドアロン型コンピューティングデバイスにも適用できる。

【００２９】

分散型コンピューティングは、コンピューティングデバイスとシステム間で直接にやりとりすることにより、コンピュータリソースとサービスの共有を容易にする。これらのリソースとサービスは、情報をやりとりすること、キャッシュ記憶、およびファイルのディスク記憶を含む。分散型コンピューティングは、ネットワーク接続性を利用して、クライアントが集団の力を生かして企業全体に利益をもたらすことを可能にする。この点に関して、種々のデバイスは、トラステッドグラフィックスパイプライン（ｔｒｕｓｔｅｄ　ｇｒａＰｈｉｃｓ　ＰｉＰｅｌｉｎｅ）に対する本発明の認証手法に関係するためにやりとりをするアプリケーション、オブジェクトまたはリソースを有することができる。

【００３０】

図２は、例示のネットワーク化されたまたは分散型コンピューティング環境を示す概略図である。分散型コンピューティング環境は、コンピューティングオブジェクト１０ａ、１０ｂなど、およびコンピューティングオブジェクトまたはデバイス１１０ａ、１１０ｂ、１１０ｃなどを含んでいる。これらのオブジェクトは、プログラム、メソッド、データストア、プログラマブルロジックなどを備える。オブジェクトは、ＰＤＡ、テレビジョン、ＭＰ３プレーヤ、パーソナルコンピュータなどの同一または異なるデバイスの部分を備えることもできる。各オブジェクトは、通信ネットワーク１４を介して他のオブジェクトと通信することができる。このネットワーク自体は、図２のシステムにサービスを提供する他のコンピューティングオブジェクトとコンピューティングデバイスとを含むことができる。本発明の一側面によれば、各オブジェクト１０または１１０は、トラステッドグラフィックスパイプラインに対する本発明の認証手法を要求できるアプリケーションを含むことができる。

【００３１】

また、当然に理解されるように、１１０ｃのようなオブジェクトは、別のコンピューティングデバイス１０または１１０上でホストとなることができる。従って、図示の物理的な環境は、接続されたデバイスがコンピュータとして示されているが、この図示は単なる例示であり、物理的な環境を、ＰＤＡ、テレビジョン、ＭＰ３プレーヤなどの種々のデジタルデバイス、インタフェース、ＣＯＭオブジェクトなどのソフトウェアオブジェクトを含むものとして、図示しまたは記載することもできる。

【００３２】

分散型コンピューティング環境をサポートするシステム、コンポーネント、およびネットワーク構成は、さまざまなものがある。例えば、コンピューティングシステムは、ワイヤライン（有線）またはワイヤレス（無線）システムによって、ローカルネットワークまたは広域分散型ネットワークによって接続される。現在では、ネットワークの多くがインターネットに結合され、インターネットが広域分散型コンピュータのインフラストラクチャを提供し、そこには多種類のネットワークが収容されている。

【００３３】

ホームネットワーキング環境では、少なくとも４種類のネットワーク伝送媒体があり、それらは、パワーライン、データ（ワイヤレスとワイヤドの両方）、音声（例えば、電話）およびエンターテイメントメディアなどの、独自のプロトコルをサポートすることができる。電灯スイッチ、家庭用電気器具などの大部分のホームコントロールデバイスは、パワーラインを使用して接続することができる。データサービスは、ブロードバンド（例えば、ＤＳＬまたはケーブルモデムのどちらか）として家庭に入ることができ、ワイヤレス（例えば、ＨｏｍｅＲＦまたは８０２．１１ｂ）またはワイヤド（例えば、Ｈｏｍｅ　ＰＮＡ、Ｃａｔ　５、普通の電源線）のどちらかで家庭内にアクセス可能である。音声トラフ

ィックは、ワイヤド（例えば、Ｃａｔ　３）としても、ワイヤレス（例えば、セル電話）としても家庭に入ることができ、Ｃａｔ　３ワイヤリングを使用して家庭内に配信することができる。エンターテインメントメディアは、衛星またはケーブルを通して家庭に入ることができ、典型的には、同軸ケーブルを使用して家庭内に配信される。ＩＥＥＥ　１３９４とＤＶＩも、メディアデバイスのクラスタをデジタル相互接続するものとして出現している。

これらネットワーク環境およびプロトコル標準として出現するかもしれない他のネットワーク環境のすべては、イントラネットを構築するように相互接続することができ、イントラネットは、インターネットを通して外部世界と接続することができる。以上を要約すると、データを格納し、伝送するための様々な異なる種類のソースが存在し、その結果、今後の動向として、コンピューティングデバイスは、データ処理パイプラインのすべての部分でコンテンツを保護する方法が必要になる。

【００３４】

インターネットとは、コンピュータネットワーキングの分野では周知である、一組のＴＣＰ／ＩＰプロトコルを利用するネットワークとゲートウェイとの集合と言われている。ＴＣＰ／ＩＰは、「ＴｒａｎＳＰｏｒｔ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｆａｃｅ　Ｐｒｏｇｒａｍ」を表す略語である。インターネットは、ユーザがネットワーク上で情報をやりとりし、共有することができるネットワーキングプロトコルを実行するコンピュータにより相互接続されている、地理的に分散されたリモートコンピュータネットワークと言うことができる。情報共有がこのように広範囲にわたっているため、インターネットなどのリモートネットワークは、広くオープンシステムになるまで発達し、ここで、開発者は、特殊なオペレーションまたはサービスを実行するためのソフトウェアアプリケーションを、ほとんど制約なしで開発することができる。

【００３５】

従って、ネットワークインフラストラクチャは、クライアント／サーバ、ピアツーピア、またはハイブリッドアーキテクチャなどのネットワークトポロジのホストを可能にする。ここで「クライアント」は、あるクラスまたはグループのメンバであり、そのクラスまたはグループとは関係のない別のクラスまたはグループのサービスを利用するものである。従って、コンピューティングの分野では、クライアントは、別のプログラムから提供されるサービスを要求するプロセス、大雑把に言うと、命令またはタスクが集まったプロセスである。クライアントプロセスは、要求したサービスを利用するとき、他方のプログラムまたはサービス自体について動作の詳細を「知っている」必要はない。クライアント／サーバアーキテクチャにおいて、特に、ネットワーク化されたシステムでは、クライアントは、別のコンピュータ、例えばサーバによって提供される共有ネットワーク資源にアクセスするコンピュータである。図２の例では、コンピュータ１１０ａ、１１０ｂなどは、クライアントと考えることができ、コンピュータ１０ａ、１０ｂなどは、サーバと考えることができ、ここで、サーバ１０ａ、１０ｂは、クライアントコンピュータ１１０ａ、１１０ｂなどに複製されたデータを維持している。

【００３６】

サーバは、典型的には、インターネットなどのリモートネットワーク上でアクセス可能なリモートコンピュータシステムである。クライアントプロセスは、第１のコンピュータシステムでアクティブにしておくことができ、サーバプロセスは、第２のコンピュータシステムでアクティブにしておくことができ、通信媒体を通して相互に通信することにより、機能を分散させることができ、複数のクライアントがサーバの情報収集能力を利用することができる。

【００３７】

クライアントとサーバは、プロトコル層に提供されている機能を利用して相互に通信する。例えば、ＨＴＴＰ（ＨｙＰｅｒｔｅｘｔ－ＴｒａｎＳｆｅｒ　Ｐｒｏｔｏｃｏｌ）は、ワールドワイドウェブ（ＷＷＷ）に関連して使用される共通プロトコルである。典型的には、ＵＲＬ（Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）またはＩＰ（Ｉ

ｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスなどのコンピュータネットワークアドレスは、サーバコンピュータまたはクライアントコンピュータであることを相互に知らせるために使用される。ネットワークアドレスは、ＵＲＬアドレスと呼ばれることもある。例えば、通信は、通信媒体上で行うことができる。具体的には、クライアントとサーバは、大容量通信用のＴＣＰ／ＩＰコネクションを通して相互に結合することができる。

【００３８】

従って、図２は、本発明を使用することができる例示のネットワーキングまたは分散型環境を示し、ここで、サーバは、ネットワーク／バスを通してクライアントコンピュータと通信している。より具体的には、複数のサーバ１０ａ、１０ｂなどは、ＬＡＮ、ＷＡＮ、イントラネット、インターネットなどとすることができる通信ネットワーク／バス１４を介して相互に接続され、ここには、ポータブルコンピュータ、ハンドヘルドコンピュータ、シンクライアント、ネットワーク化された家庭電気器具など、またはＶＣＲ、ＴＶ、オーブン、ライト、ヒータ、本発明にかかる他のデバイスなど複数のクライアントまたはリモートコンピューティングデバイス１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅなどがある。従って、本発明は、信用されたソースからのセキュアコンテンツを処理し、格納し、またはレンダリングするときに望ましい、あらゆるコンピューティングデバイスにも適用することができる。

【００３９】

通信ネットワーク／バス１４が、例えば、インターネットであるネットワーク環境において、サーバ１０は、クライアント１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅなどが、ＨＴＴＰなどの、いくつかの公知プロトコルのいずれかで通信するＷｅｂサーバにすることができる。サーバ１０は、分散型コンピューティング環境の特徴であるように、クライアント１１０となることもできる。

通信は、該当する場合には、ワイヤドにすることも、ワイヤレスにすることもできる。クライアントデバイス１１０は、通信ネットワーク／バス１４を介して通信することもあれば、通信しないこともあり、また、独立の通信を関連付けることもできる。例えば、ＴＶまたはＶＣＲの場合には、その制御にはネットワーク化された側面がある場合と、ない場合とがある。各々のクライアントコンピュータ１１０とサーバコンピュータ１０とは、種々のアプリケーションプログラムモジュールまたはオブジェクト１３５を備え付け、様々な種類の記憶要素またはオブジェクトへの接続またはアクセスを備えることができるので、これらにまたがってファイルを格納したり、またはファイルの部分をそこにダウンロードしまたは移動することができる。従って、本発明は、コンピュータネットワーク／バス１４にアクセスして、やりとりすることができるクライアントコンピュータ１１０ａ、１１０ｂなどと、クライアントコンピュータ１１０ａ、１１０ｂなど、他のデバイス１１１およびデータベース２０とやりとりすることができるサーバコンピュータ１０ａ、１０ｂなどとが置かれているコンピュータネットワーク環境で利用することができる。

【００４０】

（デジタル権利管理（ＤＲＭ）の概要）

図１３を参照して説明すると、デジタル権利管理（ＤＲＭ）と実施とは、デジタルオーディオ、デジタルビデオ、デジタルテキスト、デジタルデータ、デジタルマルチメディアなどのデジタルコンテンツ１２に関して高く望まれており、ここで、そのデジタルコンテンツ１２は、ユーザに配信される。ユーザによって受信されると、そのユーザは、メディアプレーヤなどの適当なレンダリングデバイスを、パーソナルコンピュータ１４などで使用して、そのデジタルコンテンツをレンダリングまたは「プレイ」する。

【００４１】

典型的には、このようなデジタルコンテンツ１２を配信するコンテンツ所有者または開発者（以下、「所有者」と呼ぶ）は、配信されたデジタルコンテンツ１２をユーザがどのように扱うかを制限することを望んでいる。例えば、コンテンツ所有者は、ユーザがそのコンテンツ１２をコピーし、それを第２のユーザに再配信するのを制限したいと望む場合もあれば、配信されたデジタルコンテンツ１２を、制限された回数だけ、ある時間だけ、あ

る装置の種類だけ、あるメディアプレーヤの種類だけ、あるユーザの種類だけプレイできるようにすることを望む場合がある。

【００４２】

しかし、配信が行われた後では、そのコンテンツ所有者は、デジタルコンテンツ１２を制御できても、非常に限られている。ＤＲＭシステム１０は、任意の形体のデジタルコンテンツ１２のレンダリングまたはプレイを制御下で行うことができ、ここで、この制御を、フレキシブルにし、デジタルコンテンツのコンテンツ所有者によって定義することができる。典型的には、コンテンツ１２は、任意の適当な配信チャネルを通してパッケージ１３の形でユーザに配信される。配信されるデジタルコンテンツパッケージ１３は、対称暗号化／平文化鍵（ＫＤ）（つまり、（ＫＤ（ＣＯＮＴＥＮＴ））を使用して暗号化されたデジタルコンテンツ１２が、そのコンテンツ、そのコンテンツのライセンスを取得する方法などを示している他の情報とともに含まれている。

【００４３】

信用ベースのＤＲＭシステムは、デジタルコンテンツ１２の所有者が、そのデジタルコンテンツ１２がユーザのコンピューティングデバイス１４上でレンダリングされるのを許可される前に、満足しなければならないライセンスルールを指定することができる。このライセンスルールは、上述した時間的要件を含めておくこともでき、ユーザ／ユーザのコンピューティングデバイス１４（以下、この用語は別段の断りがない限り、同じ意味で使用される）が、コンテンツ所有者またはその代理人から取得しなければならないデジタルライセンス１６の中で具現化することもできる。このライセンス１６は、デジタルコンテンツを解読するための平文化鍵（ＫＤ）を含み、おそらくは、ユーザのコンピューティングデバイスによって解読可能な鍵に従って暗号化されている。

【００４４】

デジタルコンテンツ１２の一部分のコンテンツ所有者は、ユーザのコンピューティングデバイス１４が、ライセンス１６の中でそのコンテンツ所有者により指定されたルールと要求条件に従うこと、つまり、ライセンス１６内のルールと要求条件が満たされていなければ、デジタルコンテンツ１２がレンダリングされないことを信用しなければならない。好ましくは、ユーザのコンピューティングデバイス１４は、そのデジタルコンテンツ１２に関連し、ユーザによって取得されたライセンス１６に具現化されているライセンスルールに従う場合を除き、デジタルコンテンツ１２をレンダリングすることがない信用されたコンポーネントまたは機構１８を装備している。

【００４５】

信用されたコンポーネント１８は、典型的には、ライセンス１６が有効か否かを判断し、有効とされたライセンス１６内のライセンスルールと要求条件をレビューし、レビューしたライセンスルールと要求条件に基づいて、要求側ユーザが、要求されたデジタルコンテンツ１２を、要求された方法でレンダリングする権利を有しているか否かを、判断するライセンスエバリュエータ２０を備えている。当然に理解されるように、ライセンスエバリュエータ２０は、ＤＲＭシステム１０で、デジタルコンテンツ１２の所有者の要求を、ライセンス１６内のルールと要求条件に従って履行するものと信用されており、ユーザは、悪意の有無に関係なく、あらゆる目的に信用されたエレメントを容易に変更することができないはずである。

【００４６】

当然に理解されるように、ライセンス１６内のルールと要求条件は、ユーザがデジタルコンテンツ１２をレンダリングする権利を有しているか否かを、ユーザはだれであるか、ユーザはどこにいるか、ユーザはどの種類のコンピューティングデバイスを使用しているか、どのレンダリングアプリケーションがＤＲＭシステムをコールするのか、日付、時間などの、いくつかの因子に基づいて指定することができる。さらに、ライセンス１６のルールと要求条件は、例えば、あらかじめ決めたプレイの回数、あらかじめ決めたプレイ時間にライセンス１６を制限することもできる。

【００４７】

ルールと要求条件を、任意の適当な言語とシンタックスに従ってライセンス１６に指定することができる。例えば、言語は、満足しなければならない属性と値を指定するだけのこともあれば（例えば、ＤＡＴＥ ｍｕｓｔ ｂｅ ｌａｔｔｅｒ ｔｈａｎ Ｘ）、特定のスクリプトに従って関数の実行を要求することもある（例えば、ＩＦ ＤＡＴＥ ｇｒｅａｔｅｒ ｔｈａｎ Ｘ． ＴＨＥＮ ＤＯ．．．．）。

【００４８】

ライセンス１６が有効であり、ユーザがライセンスのルールと要求条件を満足しているとライセンス工パリュエータ２０が判断すると、デジタルコンテンツ１２を、レンダリングすることができる。具体的には、コンテンツ１２をレンダリングするには、平文化鍵（ＫＤ）がライセンス１２から取得され、コンテンツパッケージ１３からの（ＫＤ（ＣＯＮＴＥＮＴ））に適用され、その結果として実際のコンテンツ１２が得られ、その実際のコンテンツ１２が実際にレンダリングされることになる。

【００４９】

（デジタルコンテンツの公表）

図３は、デジタルコンテンツを公表するための本発明にかかるシステムと方法の好適実施形態を示す機能ブロック図である。本明細書で用いられている「公表」という用語は、アプリケーションまたはサービスが、そのコンテンツに対してエンティティが発行できる権利と条件の集まりを、信用されたエンティティと共に設定し、その権利と条件をだれに発行できるかを設定するプロセスのことである。本発明によれば、公表プロセスは、デジタルコンテンツを暗号化し、コンテンツの作成者が可能な限りすべてのコンテンツユーザのために意図した永続的な実施可能権利のリストを関連付けることを含む。このプロセスを、コンテンツの作成者が意図している場合を除き、権利のいずれかへのアクセスまたはコンテンツへのアクセスを禁止するようにセキュアに実行することができる。

【００５０】

本発明の好適実施形態では、セキュアなデジタルコンテンツを公表するために、特に３つのエンティティを採用することができる。すなわち、クライアント３００側で実行され、公表されるコンテンツを準備するコンテンツ準備アプリケーション３０２、クライアントデバイス３００側に置かれているデジタル権利管理（ＤＲＭ）アプリケーションプログラムインタフェース（ＡＰＩ）３０６、および通信ネットワーク３３０を通して通信できるようにクライアント３００に結合されているＤＲＭサーバ３２０である。本発明の好適実施形態では、通信ネットワーク３３０は、インターネットを含むが、当然に理解されるように、通信ネットワーク３３０は、例えば、所有権のあるイントラネットなどのローカルまたは広域ネットワークにすることもできる。

【００５１】

コンテンツ準備アプリケーション３０２は、デジタルコンテンツを作成するあらゆるアプリケーションとすることができる。例えば、このアプリケーション３０２は、デジタルテキストファイル、デジタルミュージック、ビデオ、または他の類似コンテンツを作成するワードプロセッサ、他の出版者とすることができる。コンテンツは、例えば、ライブイベント、テープ記録されたイベントのストリーム化オーディオ／ビデオなど、ストリーム化されたコンテンツを含むこともできる。本発明によれば、コンテンツ準備アプリケーションは、ユーザが用意した鍵を使用して、そのユーザがコンテンツを暗号化することを奨励する。アプリケーション３０２は、その鍵を使用してデジタルコンテンツを暗号化し、その結果として暗号化デジタルファイル３０４を形成する。クライアントアプリケーションは、ユーザがデジタルコンテンツファイル３０４の権利データを用意することを奨励する。権利データは、デジタルコンテンツの権利を有する各エンティティのＩＤが含まれている。このエンティティは、例えば、個人、あるクラスの個人、またはデバイスにすることができる。各エンティティの権利データは、コンテンツ内にエンティティが有する権利のリストと、その権利の一部または全部に課されている条件とを含む。この権利は、デジタルコンテンツを読み取り、編集し、コピーし、印刷するなどの権利を含むことができる。さらに、権利は、包含的にも、排他的にもすることができる。包含的権利は、特定のユー

ザがコンテンツに特定の権利を有することを示している（例えば、ユーザはデジタルコンテンツを編集することができる）。排他的権利は、特定のユーザが特定の権利を除き、コンテンツにすべての権利を有することを示している（例えば、ユーザはコピーすること以外は、デジタルコンテンツに対して何でも行うことができる）。

【００５２】

本発明の一実施形態によれば、クライアントＡＰＩ３０６は、暗号化デジタルコンテンツと権利データをＤＲＭサーバ３２０に渡すことができる。以下に詳しく説明されているプロセスを使用して、ＤＲＭサーバ３２０は、ユーザが割り当てた権利を実施できるかどうかを判断し、そうであれば、ＤＲＭサーバ３２０は権利データに署名し、署名付き権利ラベル（ＳＲＬ）３０８を形成する。なお、一般的には、信用された エンティティは、好ましくはＤＲＭサーバ３２０により信用された鍵を使用して、権利データに署名することができる。例えば、クライアントは、ＤＲＭサーバ３２０から与えられた鍵を使用して権利データに署名することができる。

【００５３】

権利ラベル３０８は、権利の記述を表わすデータ、暗号化コンテンツ鍵、および権利記述と暗号化コンテンツ鍵に対するデジタル署名とを含むことができる。

ＤＲＭサーバが権利ラベルに署名する場合には、ＤＲＭサーバは、署名付き権利ラベル３０８をクライアントＡＰＩ３０６経由でクライアントに送り返し、署名付き権利ラベル３０８をクライアントデバイス３００に格納する。コンテンツ準備アプリケーション３０２は、署名付き権利ラベル３０８を暗号化デジタルコンテンツファイル３０４と関連付ける。例えば、ＳＲＬ３０８を、暗号化デジタルコンテンツファイルと連結し、権利管理コンテンツファイル３１０を生成する。

なお、一般的には、権利データは、デジタルコンテンツと結合する必要はない。

例えば、権利データを、既知のロケーションに格納しておくことができ、格納された権利データのレファレンスを、暗号化デジタルコンテンツと結合することができる。このレファレンスは、権利データがどこに格納されているかを示す識別子（例えば、権利データを含むデータストア）、およびその特定のストレージのロケーションに置かれている、その特定の権利データに対応する識別子（例えば、関心のある特定の権利データが置かれているファイルを特定するもの）を含むことができる。権利管理コンテンツ３１０は、どこにいてもだれにでも配信することができ、コンテンツを消費する権利を有するエンティティだけが、コンテンツを消費することができ、しかも、そのエンティティに割り当てられた権利に従ってのみコンテンツを消費することができる。

【００５４】

図４は、権利管理デジタルコンテンツを公表するための本発明による例示方法４００を示すフローチャートであり、ここで、権利ラベルは、ＤＲＭサーバによって署名されている。なお、当然に理解されるように、この実施形態は、単なる例示であり、権利ラベルを、一般的には、あらゆる信用された エンティティによって署名することができる。一般的には、デジタルコンテンツを公表するための本発明による方法は、コンテンツ鍵（ＣＫ）を使用してデジタルコンテンツを暗号化し、デジタルコンテンツに関連する権利記述を生成し、ＤＲＭサーバの公開鍵（ＰＵ－ＤＲＭ）に従ってコンテンツ鍵（ＣＫ）を暗号化して、その結果として（ＰＵ－ＤＲＭ（ＣＫ））が得られるようにし、権利記述と（ＰＵ－ＤＲＭ（ＣＫ））との結合に対して（ＰＵ－ＤＲＭ）に対応する秘密鍵（ＰＲ－ＤＲＭ）に基づいて、デジタル署名を生成することを含むことができる。

【００５５】

ステップ４０２において、アプリケーション３０２は、デジタルコンテンツを暗号化するために使用されるコンテンツ鍵（ＣＫ）を生成する。好ましくは、コンテンツ鍵（ＣＫ）は対称鍵になっているが、一般的には、どの鍵を使用してもデジタルコンテンツを暗号化することができる。対称鍵アルゴリズムは、「秘密鍵」アルゴリズムと呼ばれることもあるが、メッセージを暗号化するときに使用した同じ鍵を使用して、メッセージを解読する。そのような理由から、（ＣＫ）は秘密に保っていることが好ましい。送信側と受信側の

間で（ＣＫ）を共有することは、（ＣＫ）が無許可でインターセプトされるのを防止するために、慎重に行う必要がある。（ＣＫ）は、暗号化する側と解読する側の両方で共有されるので、（ＣＫ）は、好ましくは、暗号化されたメッセージが送信される前に通知される。

【００５６】

この分野では、いくつかの対称鍵生成アルゴリズムがよく知られている。好適実施形態では、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）が採用されるが、当然に理解されるように、どの対称鍵アルゴリズムも使用することができる。このような対称鍵アルゴリズムの例を挙げると、これらに限定されないが、ＴｒｉＰｌｅ－ＤＥＳ、ＩＤＥＡ（ｔｈｅ　Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ａｌｇｏｒｉｔｈｍ）、Ｃａｓｔ、Ｃａｓｔ－１２８、ＲＣ４、ＲＣ５、ＳｋｉＰＪａｃｋがある。

【００５７】

ステップ４０４において、アプリケーション３０２は、対称コンテンツ鍵（ＣＫ）を使用してデジタルコンテンツを暗号化し、暗号化デジタルコンテンツ３０４を形成する。これは、（ＣＫ（ｃｏｎｔｅｎｔ））という表記を使用して書かれている。アプリケーション３０２を使用する作成者は、デジタルコンテンツに関連する権利データを生成することもできる。権利データは、コンテンツを消費する権利があるエンティティのリストと、コンテンツに対してエンティティの各々が所有している特定の権利とを、その権利に課されている条件とともに含むことができる。この権利は、例えば、コンテンツを表示すること、コンテンツを印刷することなどを含むことができる。アプリケーション３０２は、権利データをＡＰＩ３０６に渡す。ＸＭＬ／ＸｒＭＬフォーマットの権利データの例は、付録１として本明細書に添付されている。

【００５８】

ステップ４０６において、ＡＰＩ３０６は、第２の暗号化鍵（ＤＥＳ１）を生成する。これは、コンテンツ鍵（ＣＫ）を暗号化するために使用される。好ましくは、（ＤＥＳ１）は対称鍵である。ステップ４０８において、ＡＰＩ３０６は、（ＤＥＳ１）を使用して（ＣＫ）を暗号化し、その結果として（ＤＥＳ１（ＣＫ））を得る。ステップ４１０において、ＡＰＩ３０６は（ＣＫ）を破棄するので、（ＣＫ）は、（ＤＥＳ１（ＣＫ））を解読することによってのみ取得できるようになる。（ＣＫ（ｃｏｎｔｅｎｔ））が中央のＤＲＭサーバ３２０に対して保護されること、およびコンテンツに対するすべての「ライセンス要求」が権利データに従って行われることを保証するために、ＡＰＩ３０６は、ステップ４１２において、用意されているＤＲＭサーバ３２０に連絡し、公開鍵（ＰＵ－ＤＲＭ）を取り出す。ステップ４１４において、ＡＰＩ３０６は、（ＰＵ－ＤＲＭ）を使用して（ＤＥＳ１）を暗号化し、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得る。従って、（ＣＫ）は、（ＰＵ－ＤＲＭ）に対して保護され、（ＣＫ（ｃｏｎｔｅｎｔ））を解読する必要が起こったとき、ＤＲＭサーバ３２０が（ＣＫ）にアクセスできる唯一のエンティティとなることを保証することができる。ステップ４１６において、ＡＰＩ３０６は、（ＤＥＳ１）を使用して権利データ（つまり、許可された各エンティティのリストと、リスト内の許可された各エンティティに関連する権利と条件）を暗号化し、その結果として（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を得る。

【００５９】

別の実施形態では、（ＣＫ）を使用して、権利データを直接に暗号化し、その結果として（ＣＫ（ｒｉｇｈｔｓｄａｔａ））を得るので、（ＤＥＳ１）の使用を完全に無くすことができる。しかし、権利データを暗号化するために（ＤＥＳ１）を使用すると、ＤＲＭサーバに従う特定のアルゴリズムに、その（ＤＥＳ１）を適合させることが可能になるが、他方、（ＣＫ）は、ＤＲＭサーバから独立したエンティティによって指定され、ＤＲＭサーバに準拠しないことになる。

【００６０】

ステップ４１８において、コンテンツ保護アプリケーション３０２は、署名のための権利

ラベルとして、（ＰＵ－ＤＲＭ（ＤＥＳ１））と（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））とをＤＲＭサーバに提出することができる。別の方法として、クライアント自身が、権利データに署名することもできる。権利データが署名のためにサーバに提出される場合には、ステップ４２０において、ＤＲＭサーバ３２０は、権利データにアクセスし、提出された権利ラベル内の権利と条件を実施できることを確認する。権利データを実施できることを確認するために、ＤＲＭサーバ３２０は、（ＰＲ－ＤＲＭ）を（ＰＵ－ＤＲＭ（ＤＥＳ１））に適用し、その結果として（ＤＥＳ１）を得て、（ＤＥＳ１）を（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））に適用し、その結果として平文の権利データを得る。次に、サーバ３２０は、いずれかのポリシチェックを行って、権利データに指定されているユーザ、権利、および条件がサーバ３２０によって実施されたポリシの範囲内にあることを確かめることができる。サーバ３２０は、（ＰＵ－ＤＲＭ（ＤＥＳ１））と（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））とを含んでいる、最初に提出された権利データに署名し、その結果として署名付き権利ラベル（ＳＲＬ）３０８を得る。ここで、署名は、ＤＲＭサーバ３２０の秘密鍵（ＰＲ－ＤＲＭ）に基づいており、ＳＲＬ３０８をＡＰＩ３０６に送り返し、戻されたＳＲＬ３０８をクライアントアプリケーション３０２に提示する。

【００６１】

ＳＲＬ３０８は、デジタル署名されたドキュメントであり、不正行為に強くなっている。さらに、ＳＲＬ３０８は、コンテンツを暗号化するために使用された実際の鍵のタイプとアルゴリズムから独立しているが、ＳＲＬ３０８が保護しているコンテンツと強い１対１の関係を保っている。図５に示すように、本発明の一実施形態では、ＳＲＬ３０８は、おそらくコンテンツのＩＤを含む、ＳＲＬ３０８の基礎となっているコンテンツに関する情報と、（ＰＵ－ＤＲＭ（ＤＥＳ１））を含む、ＳＲＬ３０８に署名したＤＲＭサーバに関する情報と、ネットワーク上のＤＲＭサーバを見つけるためのＵＲＬなどの照会情報、およびＵＲＬが失敗したときのフォールバック情報と、ＳＲＬ３０８自体を記述している情報と、（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））：（ＤＥＳ１（ＣＫ））と、Ｓ（ＰＲ－ＤＲＭ）とを含むことができる。ＸＭＬ／ＸｒＭＬにおけるＳＲＬ３０８の例は、付録２として本明細書に添付されている。

【００６２】

信用された工ンティティは、権利データに署名して、署名付き権利ラベル３０８を生成することを確かめることによって、ＤＲＭサーバは、権利ラベル３０８の権利データに記述されているように出版者によって規定された項目に従って、コンテンツに対するライセンスを発行することを主張する。当然に理解されるように、ユーザは、特にライセンスがコンテンツ鍵（ＣＫ）を含んでいるために、コンテンツをレンダリングするためのライセンスを取得することが要求される。

ユーザが暗号化コンテンツに対するライセンスを取得したいときには、ユーザは、コンテンツに対するＳＲＬ３０８と、ユーザの信用証明物を検証する証明書を含むライセンス要求を、ＤＲＭサーバ３２０または他のライセンス発行エンティティに提示することができる。ライセンス発行エンティティは、（ＰＵ－ＤＲＭ（ＤＥＳ１））と（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））とを解読し、権利データを生成して、作成者（存在する場合）によってライセンス発行エンティティに許可されたすべての権利をリストし、その特定権利だけを含むライセンスを構築することができる。

【００６３】

好ましくは、アプリケーション３０２がＳＲＬ３０８を受け取ると、そのアプリケーション３０２は、署名付き権利ラベル３０８を対応する（ＣＫ（ｃｏｎｔｅｎｔ））３０４と連結し、権利管理デジタルコンテンツを形成する。別の方法として、権利データを、暗号化デジタルコンテンツが提供されているロケーションのレファレンスとともに、そのロケーションに格納することができる。従って、ＤＲＭ対応のレンダリングアプリケーションは、そのレンダリングアプリケーションがレンダリングしようとしているコンテンツ部分を通して、署名付き権利ラベル３０８を見つけることができる。署名付き権利ラベルが見つかると、レンダリングアプリケーションをトリガし、ＤＲＭサーバ３２０に対してライ

センス要求を開始する。公表アプリケーション３０２は、例えば、ＤＲＭライセンスサーバ３２０にＵＲＬを格納することができるが、ＤＲＭライセンスサーバは、権利ラベルにデジタル署名する前に、自身のＵＲＬをメタデータの一部として権利ラベルに組み込むことができ、レンダリングアプリケーションによってコールされたＤＲＭクライアントＡＰＩ３０６は、正しいＤＲＭライセンスサーバ３２０を特定することができる。好ましくは、例えば、ＧＵＩＤ（ｇｌｏｂａｌｌｙ ｕｎｉｑｕｅ ｉｄｅｎｔｉｆｉｅｒ）などのユニーク識別子は、その署名の前に権利ラベルに組み入れられている。

【００６４】

本発明の好適実施形態では、ＳＯＡＰ（ｓｉｍｐｌｅ ｏｂｊｅｃｔ ａｃｃｅｓｓ ｐｒｏｔｏｃｏｌ）を使用して、コンテンツ保護アプリケーション３０２またはレンダリングアプリケーションとＤＲＭサーバ３２０との間の通信を行うことができる。さらに、ＡＰＩ３０６などのＡＰＩライブラリを用意しておけば、アプリケーション３０２などのアプリケーションは、ＤＲＭプロトコルのクライアント側に実装する必要がなくなり、ローカルＡＰＩコールを行うだけで済むようになる。好ましくは、ＸｒＭＬ、ＸＭＬ言語を使用して、権利記述、ライセンス、およびデジタルコンテンツの権利ラベルを記述するが、当然に理解されるように、適当なフォーマットを、権利記述と他のデータに使用することができる。

【００６５】

（公表されるコンテンツのライセンスの取得）

図６は、権利管理デジタルコンテンツをライセンシングするための本発明にかかるシステムと方法の好適実施形態を示す機能ブロック図である。本明細書で用いられている「ライセンシング」という用語は、ライセンスの中で指名された エンティティが、ライセンスに規定された条項に従ってコンテンツを消費するのを可能にするライセンスを要求し、および受け取るために、アプリケーションまたはサービスが従うプロセスのことである。ライセンスプロセスへの入力は、ライセンスを要求されたコンテンツに関連する署名付き権利ラベル（ＳＲＬ）３０８、およびライセンスを要求されたエンティティの公開鍵証明書を含むことができる。当然に理解されるように、ライセンスを要求するエンティティは、必ずしも、ライセンスを要求されたエンティティである必要はない。典型的には、ライセンスは、ＳＲＬ３０８からの権利記述、暗号化コンテンツを解読できる暗号化鍵、および権利記述と暗号化鍵に対するデジタル署名を含む。デジタル署名は、指名されたエンティティと権利が合法的であることを示している。

【００６６】

アプリケーション３０２が権利管理コンテンツ３１０を消費する１つの方法は、クライアントＡＰＩ３０６が、権利管理コンテンツ３１０の署名付き権利ラベル３０８を、通信ネットワーク３３０を介してＤＲＭサーバ３２０に転送することである。ＤＲＭサーバ３２０が置かれているロケーションは、例えば、ＳＲＬ３０８の照会情報の中に見つけることができる。このような実施形態では、ＤＲＭライセンシングサーバ３２０は、以下に詳しく説明されているプロセスを通して、権利ラベルの中の権利記述を使用してライセンスを発行できるか否かを判断し、そうであれば、ライセンスに含まれる権利記述を取り出すことができる。上述したように、権利ラベル３０８は、ＤＲＭサーバ３２０の公開鍵（ＰＵ－ＤＲＭ）に従って暗号化されたコンテンツ鍵（ＣＫ）（すなわち、（ＰＵ－ＤＲＭ（ＣＫ））を含む。ライセンスを発行するプロセスにおいて、ＤＲＭサーバ３２０は、この値をセキュアに解読して（ＣＫ）を取得する。そのあと、ライセンス要求において渡された公開鍵証明書の公開鍵（ＰＵ－ＥＮＴＩＴＹ）を使用して、（ＣＫ）を再暗号化する（すなわち、（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））。新たに再暗号化された（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））は、サーバ３２０がライセンスに入れるものである。従って、ライセンスを、関連する秘密鍵（ＰＲ－ＥＮＴＩＴＹ）の所持者だけが（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））から（ＣＫ）を回復できるので、（ＣＫ）が公表されるリスクなしに、コール側に戻すことができる。次に、クライアントＡＰＩ３０６は（ＣＫ）を使用して、暗号化コンテンツを解読し、解読されたデジタルコンテンツ３１２を形成する。クライアントアプリケ

ーション３０２は、ライセンスに提供されている権利に従って、解読されたデジタルコンテンツ３１２を使用することができる。

【００６７】

別の方法として、例えば、公表クライアントなどのクライアントは、コンテンツを消費するために独自のライセンスを発行することもできる。このような実施形態では、セキュアされたプロセスを、適当な状況の下でデジタルコンテンツを解読するために必要な鍵をクライアントに提供するクライアントコンピュータ上で実行することができる。

【００６８】

図７と図８は、権利管理デジタルコンテンツをライセンシングするための本発明によるシステムと方法の好適実施形態のフローチャートを示す図である。本発明によれば、要求側のエンティティは、１または複数の潜在的ライセンシに代わってライセンス要求を提出することができる。潜在的ライセンシとしては、人、グループ、デバイス、またはなんらかの方法でコンテンツを消費できる他のエンティティなどがある。以下に説明する方法６００の実施形態では、ＤＲＭサーバがライセンス要求を処理するようになっているが、当然に理解されるように、ライセンス要求処理をクライアント側で行い、ライセンスをクライアントに直接に発行させることもできる。

【００６９】

ステップ６０２において、例えば、ＤＲＭサーバなどのライセンス発行エンティティは、ライセンス要求を受け取る。好ましくは、ライセンス要求は、１または複数の要求されたライセンシの各々の公開鍵証明書またはＩＤのどちらかを含む。以下に、ライセンス要求の好適実施形態のＳＯＡＰプロトコルを示す。

【００７０】

【表１】

```
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <AcquireLicense xmlns= "http://xxxx.com/PublishingService">
      <RequestParams>
        <AcquireLicenseParams>
          <LicenseeCerts>
            <String>string</String>
            <String>string</String>
          </LicenseeCerts>
          <RightsSpecification>string</RightsSpecification>
          <RightsOfferID>string</RightsOfferID >
          <ApplicationData>string</ApplicationData >
        </AcquireLicenseParams>
        <AcquireLicenseParams>
              ...
        </AcquireLicenseParams>
      </RequestParams>
    </AcquireLicense>
  </soap:Body>
</soap:Envelope>
```

【００７１】

ステップ６０４において、要求側のエンティティ（すなわち、ライセンス要求を行うエンティティ）が認証される。本発明の一実施形態によれば、ライセンス発行エンティティを、プロトコル（例えば、チャレンジ－応答）認証を使用して、要求側エンティティのＩＤを判断するように構成することも、要求側エンティティの認証を要求しないように（これ

は、「匿名認証を許容する」とも呼ばれる）構成することもできる。認証が要求される場合には、あらゆる種類の認証方式を使用することができる（例えば、上述のチャレンジー応答方式、ＭＩＣＲＯＳＯＦＴ．ＮＥＴ、ＰＡＳＳＰＯＲＴ、ＷＩＮＤＯＷＳ（登録商標）　ａｕｔｈｏｒｉｚａｔｉｏｎ、Ｘ５０９などのユーザＩＤ・パスワード方式）。好ましくは、匿名認証が許容されるとともに、統合された情報システムによってサポートされる、あらゆるプロトコル認証方式をサポートする。認証ステップの結果は、例えば、「匿名」ＩＤ（匿名認証の場合）などのＩＤであるか、またはパーソナルアカウントＩＤである。ラインセンス要求がなんらかの理由で認証できないときは、エラーが戻され、ライセンスは許可されない。

【００７２】

ステップ６０６において、認証されたエンティティが許可される。つまり、ステップ６０８で認証されたエンティティが、ライセンスを要求するのを許されているか否か（自身のためか、別のエンティティのためか）が判断される。好ましくは、ライセンス発行エンティティは、ライセンスを要求するのを許されている（または許されていない）エンティティのリストを格納する。好適実施形態では、このＩＤリストの中のＩＤは、ライセンスが要求されるエンティティのＩＤではなく、要求を行うエンティティのＩＤになっているが、どちらにすることも可能である。例えば、パーソナルアカウントＩＤは、ライセンス要求を直接に行うことが許されていないが、トラステッドサーバプロセスは、そのエンティティに代行してライセンス要求を行うことができる。

【００７３】

本発明によれば、ライセンス要求には、各潜在的ライセンシの公開鍵証明書またはＩＤのどちらも含むことができる。ライセンスが１人のライセンシのためにだけ要求されるときは、１つの証明書またはＩＤだけが指名される。ライセンスが複数のライセンシのために要求されるときは、証明書またはＩＤは、各潜在的ライセンシに対して指名される。

【００７４】

好ましくは、ライセンス発行エンティティは、有効なライセンシごとに公開鍵証明書を持っている。しかし、アプリケーション３０２は、所与のユーザにライセンスを生成することを望む場合でも、アプリケーション３０２は、そのユーザの公開鍵証明書にアクセスできないことがある。このような場合は、アプリケーション３０２は、ライセンス要求の中でユーザのＩＤを指定できるので、その結果、ラインセンス発行エンティティは、ディレクトリサービスのルックアップを実行して、該当ユーザの公開鍵証明書を戻す登録された証明書のプラグインモジュールを呼び出すことができる。

【００７５】

ステップ６０８において、発行エンティティがライセンス要求に公開鍵証明書が含まれていないと判断したときは、発行エンティティは、指定されたＩＤを使用して、ディレクトリサービスまたはデータベースのルックアップを実行して、該当する公開鍵証明書を探し出す。ステップ６１０において、発行エンティティは、証明書がディレクトリにあると判断したときは、ステップ６１２で、その証明書が取り出される。好適実施形態では、証明書プラグインを使用して、ディレクトリアクセスプロトコルを介して、ディレクトリサービスから公開鍵証明書を取り出す。所与の潜在的ライセンシの証明書を、要求またはディレクトリの中に見つけることができないときには、ライセンスサーバは、その潜在的ライセンシのライセンスを生成しないので、ステップ６１４において、エラーを要求側エンティティに戻す。

【００７６】

ライセンス発行エンティティが、少なくとも１つの潜在的ライセンシの公開鍵証明書を有すると、ステップ６１６において、発行エンティティは、ライセンシ証明書の信頼性を検証する。好ましくは、発行エンティティは、１組の信用された証明書発行者証明書を有するように構成され、ライセンシ証明書の発行者が、信用された発行者のリストにあるか否かを判断する。ステップ６１６において、発行エンティティは、ライセンシ証明書の発行者がトラステッド発行者のリストにないと判断したときには、そのライセンシに対する要

求は失敗し、ステップ６１４においてエラーが生成される。従って、信用された発行者によって発行されていない証明書を有する潜在的ライセンシは、ライセンスを受け取らない。

【００７７】
さらに、発行エンティティは、好ましくは、信用された発行者証明書から個別のライセンシの公開鍵証明書までに至る証明書チェーンの中のすべてのエンティティに対してデジタル署名の有効性検査を実行する。チェーンの中のデジタル署名の有効性を検査するプロセスは、周知のアルゴリズムである。所与の潜在的ライセンシに対する公開鍵証明書が有効でないとき、またはチェーンの中の証明書が有効でないときには、潜在的ライセンシは信用されないので、ラインセンスをその潜在的ライセンシに発行しない。そうでなければ、ステップ６１８において、ライセンスを発行する。このプロセスは、ライセンスが要求されているすべてのエンティティが処理されるまで、ステップ６２０から繰り返される。

【００７８】
図８に示すように、ライセンス発行エンティティは、ライセンス要求の中で受け取られた署名付き権利ラベル３０８の有効性検査に進む。好適実施形態では、発行エンティティは、権利ラベルプラグインとバックエンドデータベースを使用して、発行エンティティによって署名されたすべての権利ラベルのマスタコピーを、サーバに苦悩することができる。権利ラベルは、公表時に権利ラベルに入れられたＧＵＩＤで識別される。ライセンス時に（ステップ６２２）、発行エンティティは、ライセンス要求の中の権利ラベル入力を解析し、そのＧＵＩＤを取り出す。このＧＵＩＤ、権利ラベルプラグインに渡され、そこから、データベースに対するクエリが出され、マスタ権利ラベルのコピーが取り出される。マスタ権利ラベルは、ライセンス要求の中で送信された権利ラベルのコピーよりも最新であるので、以下のステップでは、これが要求の中で使用される権利ラベルとなる。権利ラベルがＧＵＩＤに基づいてデータベースに見つからないときには、発行エンティティは、ステップ６２４においてそのポリシをチェックし、要求の中の権利ラベルに基づいてライセンスを発行することがまだ許されているか否かを判断する。ポリシがこれを許していなければ、ライセンス要求は、ステップ６２６において失敗し、ステップ６２８において、エラーがＡＰＩ３０６に戻される。

【００７９】
ステップ６３０において、ライセンス発行エンティティは、権利ラベル３０８の有効性を検査する。権利ラベル上のデジタル署名が有効性検査され、ライセンス発行エンティティが権利ラベルの発行者（権利ラベルに署名したエンティティ）でなければ、ライセンス発行エンティティは、権利ラベルの発行者が別の信用された工ンティティ（つまり、鍵マテリアルをライセンス発行エンティティと共有できるエンティティ）であるか否かを判断する。権利ラベルが有効でないか、または権利ラベルが信用されたエンティティによって発行されたものでなければ、ライセンス要求は、ステップ６２６において失敗し、ステップ６２８において、エラーがＡＰＩ３０６に戻される。

【００８０】
すべての有効性検査が行われた後、ライセンス発行エンティティは、承認されたライセンシの各々に対して権利ラベル３０８をライセンスに変換する。ステップ６３２において、ライセンス発行エンティティは、各ライセンシに対して発行されるライセンスに関するそれぞれの権利記述を生成する。各ライセンシについて、発行エンティティは、そのライセンシの公開鍵証明書に指名されているＩＤを、権利ラベルの中の権利記述に指名されているＩＤと突き合わせて評価する。
権利記述は、ライセンスの権利または権利セットを行使できるＩＤセットを、すべての権利または権利セットに割り当てる。このライセンシのＩＤが関連付けられているすべての権利または権利セットについて、その権利または権利セットは、ライセンシの新しいデータ構造の中にコピーされる。その結果のデータ構造は、特定のライセンシのライセンスにおける権利記述である。このプロセスの一部として、ライセンス発行エンティティは、権利ラベルの権利記述における権利または権利セットのいずれかと関連付けられている前提

条件を評価する。例えば、権利は、時間に関する時間前提条件が関連付けられていることがあり、これは、指定した時間が経過した後、ライセンス発行エンティティがライセンスを発行するのを制限する。この場合には、発行エンティティは、現在の時間をチェックする必要があり、その時間が、前提条件の中で指定された時間を経過していれば、発行エンティティは、そのライセンシのＩＤがその権利と関連付けられていた場合でも、ライセンシに対してその権利を発行することができなくなる。

【００８１】

ステップ６３６において、発行エンティティは、権利ラベルから（ＰＵ－ＤＲＭ（ＤＥＳ１））と（ＤＥＳ１（ＣＫ））を取り出し、（ＰＲ－ＤＲＭ）を適用して（ＣＫ）を得る。

次に、発行エンティティは、ライセンシの公開鍵証明書（ＰＵ－ＥＮＴＩＴＹ）を使用して（ＣＫ）を再暗号化し、その結果として（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））を得る。

ステップ６３８において、発行エンティティは、生成された権利記述を（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））と連結し、（ＰＲ－ＤＲＭ）を使用してその結果のデータ構造にデジタル署名する。この署名付きデータ構造は、この特定ライセンシのライセンスである。

【００８２】

ステップ６４０において、発行エンティティが、特定要求に対して生成すべきライセンスが残っていないと判断したときには、ゼロまたはそれ以上のライセンスを生成したことになる。生成されたライセンスは、そのライセンスと関連付けられた証明書チェーン（例えば、サーバの独自の公開鍵証明書のほかに、その証明書を発行した証明書など）とともに、ステップ６４２において要求側エンティティに戻される。

【００８３】

以下に、ライセンス応答の好適実施形態のＳＯＡＰプロトコルを示す。

【００８４】

【表２】

```
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <AcquireLicenseResponse xmlns="http://xxxx.com/LicensingService">
      <AcquireLicenseResult>
        <AcquireLicenseResponse>
          <CertificateChain>
            <String>string</String>
            <String>string</String>
          </CertificateChain>
        </AcquireLicenseResponse>
        <AcquireLicenseResponse>
              ...
        </AcquireLicenseResponse>
            ...
      </AcquireLicenseResult>
    </AcquireLicenseResponse>
  </soap:Body>
</soap:Envelope>
```

【００８５】

本発明によるシステムの好適実施形態では、複数のライセンサ鍵を使用することができる。このような実施形態では、暗号化されて権利ラベル３０８を介してライセンスに移されるコンテンツ鍵（ＣＫ）は、実際には、どのような任意データにもすることができる。特

に有用な方法の１つは、それぞれが権利記述の中の異なる権利または異なる本人と関連付けられている、複数の別々に暗号化されたコンテンツ鍵（ＣＫ）を使用することである。例えば、アルバム上の歌曲のデジタル版は、すべてを異なる鍵（ＣＫ）で暗号化される。これら鍵（ＣＫ）は、同じ権利ラベルに含まれるが、本人は歌曲の１つをプレイする権利を有することができ（例えば、本人は、自分のライセンスの１つの鍵を取得する権利だけを有することがある）、別の人は、すべての歌曲をプレイする権利を有することができる（自分のライセンスのすべての鍵を取得する権利を有することになる）。

【００８６】

好ましくは、本発明にかかるシステムは、公表アプリケーション／ユーザが、権利ラベル３０８のライセンシのグループまたはクラスを指名することを可能にする。このような実施形態では、ライセンス発行エンティティは、権利ラベルの中で指名されたグループ／クラスを評価して、現在のライセンシＩＤが、そのグループ／クラスのメンバであるか否かを判断する。指名されたグループ／クラスのメンバであると判断されると、発行エンティティは、そのグループ／クラスに関連する権利または権利のセットを、ライセンスのために使用される権利記述データ構造に追加することができる。

【００８７】

本発明の好適実施形態では、ＤＲＭサーバの公表およびライセンスプロトコルインタフェースは、コール側アプリケーションまたはユーザの認証と許可をサポートしているので、ＤＲＭサーバの管理コンソールは、アドミニストレータが、ライセンシングと公表の両方のインタフェースに対するアクセス制御リストを生成できるようにする。このようにすると、サーバの顧客は、ユーザ／アプリケーションが、公表またはライセンス、またはその両方を行うことを許容するポリシを適用することができる。

【００８８】

（署名付き権利ラベルの修正または再公表）

本発明の一実施形態では、コンテンツのユーザが、そのようなことを行う十分な許可が与えられていれば、ＳＲＬ３０８を「再公表」することができる。すなわち、そうすることが許されていれば、ユーザは、ＳＲＬ３０８内の権利データを変更することができる。特に、このような権利データを変更する許可を、権利データを変更する許可を有するユーザが、本質的に、関連するコンテンツに対してその広範な権利を許可することができるように、控え目に、賢明に行うべきである。考えられることは、このようなユーザは、コンテンツを公表し、それを外部に転送する権利を自身に許可することができる。

【００８９】

ここでは、変更する許可は、特定のユーザまたはユーザのクラスが権利データと権利ラベル３０８とを実際に変更し、または「再公表」できるとの指示を、ＳＲＬ３０８内の権利データに含めることによって通知される。ＤＲＭサーバ３２０は、ライセンスの要求に関連してこのような許可を有するＳＲＬ３０８を受け取ると、ＤＲＭサーバ３２０は、ユーザの公開鍵（つまり、ＰＵ－ＥＮＴＩＴＹ）に従って暗号化されたユーザの対称鍵（ＤＥＳ１）が、結果として（ＰＵ－ＥＮＴＴＩＴＹ（ＤＥＳ１））となる、要求されたライセンスに含める。

【００９０】

従って、ＳＲＬ３０８内の権利データを編集するには、図９に示すように、ユーザは、ライセンスから（ＰＵ－ＥＮＴＩＴＹ（ＤＥＳ１））を取り出し（ステップ７０１）、（ＰＲ－ＥＮＴＩＴＹ）をそれに適用し、その結果として（ＤＥＳ１）を得るようにし（ステップ７０３）、ＳＲＬ３０８から（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を取り出し（ステップ７０５）、（ＤＥＳ１）をそれに適用し、その結果として権利データを得る（ステップ７０７）。そのあと、ユーザは、希望通りに権利データを変更し（ステップ７０９）、変更された権利データを、図４を参照して説明した方法でＤＲＭ３２０に提出し、署名付き権利ラベル３０８を得る（ステップ７１１）。もちろん、ここでは、署名付き権利ラベル３０８は、実際には再公表されたＳＲＬ３０８であり、ＳＲＬ３０８が受け取られた後（ステップ７１３）、ユーザは、関連するコンテンツに連結されていた元のＳＲＬ３０

８を取り除き（ステップ７１５）、その再公表されたＳＲＬ３０８を、そのコンテンツに連結する（ステップ７１７）。

【００９１】

以上から当然に理解されるように、ＳＲＬ３０８を再公表すると、ユーザは、権利、条件およびユーザを含む、ＳＲＬ３０８内の権利データを、関連コンテンツを変更せずに更新することができる。具体的には、再公表は、関連コンテンツを新しい（ＣＫ）で再暗号化する必要はない。また、再公表は、元のＳＲＬ３０８が新しいＳＲＬ３０８にコピーされる多数のアイテムを有するために、最初から新しいＳＲＬを生成する必要はない。

【００９２】

（署名付き権利ラベル３０８の自己公表）

本発明の一実施形態では、ＳＲＬ３０８は、要求側ユーザ自身によって署名することができる。従って、ユーザは、ＤＲＭサーバ３２０に連絡し、関連するコンテンツの一部分のＳＲＬ３０８を取得する必要はない。その結果、自己公表（Ｓｅｌｆ－Ｐｕｂｌｉｓｈｉｎｇ）は、オフラインの公表とも呼ばれている。このような実施形態では、ユーザは、ＤＲＭ３２０に連絡することが要求され、自己公表されたＳＲＬ３０８に基づいたライセンスを要求する。当然に理解されるように、公表エンティティは、独自のライセンスを発行することができる。

【００９３】

具体的には、図１０に示すように、この実施形態では、ユーザは、ＤＲＭサーバ３２０からＤＲＭ証明書８１０を受け取ることにより、自己公表する用意ができる。ＤＲＭ証明書８１０は、公開鍵（ＰＵ－ＣＥＲＴ）、およびユーザの公開鍵（ＰＵ－ＥＮＴＩＴＹ）に従って暗号化され、その結果として（ＰＵ－ＥＮＴＩＴＹ（ＰＲ－ＣＥＲＴ））となる対応する秘密鍵（ＰＲ－ＣＥＲＴ）とを含む。証明書は、ＤＲＭサーバ３２０の秘密鍵（ＰＲ－ＤＲＭ）で署名され、以下で詳しく説明するように、そのＤＲＭサーバ３２０がそれを検証することができる。当然に理解されるように、ＤＲＭ証明書８１０は、ユーザが自己公表するのを許可する。当然に理解されるように、鍵ペア（ＰＵ－ＣＥＲＴ，ＰＲ－ＣＥＲＴ）は、（ＰＵ－ＥＮＴＩＴＹ，ＰＲ－ＥＮＴＩＴＹ）とは別で、特に自己公表のために使用される。

なお、鍵ペア（ＰＵ－ＣＥＲＴ，ＰＲ－ＣＥＲＴ）は使用しないで済むこともあり、その場合には、ＤＲＭ証明書８１０は、ユーザの公開鍵（ＰＵ－ＥＮＴＩＴＹ）だけを含み、ＤＲＭサーバ３２０の秘密鍵（ＰＲ－ＤＲＭ）で署名され、そのＤＲＭサーバがそれを検証することができる。

【００９４】

自己公表は、ユーザがそれにより実行されるステップに関してＤＲＭサーバ３２０に代わる点で、図４に示す公表と異なっている。特に、ユーザが、提出された権利ラベルに署名し、その結果として署名付き権利ラベル（ＳＲＬ）３０８となることである。提出された権利ラベルは、ＤＲＭ証明書８１０から取得された（ＰＲ－ＣＥＲＴ）（つまり、Ｓ（ＰＲ－ＣＥＲＴ））とともに、（ＰＵ－ＤＲＭ（ＤＥＳ１））と（ＤＥＳ１（ｒｉｇｈｔｓ ｄａｔａ））とを含む。当然に理解されるように、ユーザは、ＤＲＭ証明書８１０から（ＰＵ－ＥＮＴＩＴＹ（ＰＲ－ＣＥＲＴ））を取得し、それに（ＰＲ－ＥＮＴＩＴＹ）を適用することによって、ＤＲＭ証明書８１０から（ＰＲ－ＣＥＲＴ）を取得する。ここで注意すべきことは、ユーザが（ＰＵ－ＤＲＭ（ＤＥＳ１））に適用する（ＰＲ－ＤＲＭ）を有していないために、ユーザは、ＤＲＭサーバ３２０が提出された権利ラベルの権利を実施することができるという検証をすることができない。従って、ＤＲＭサーバ３２０自身は、ライセンスが自己公表されたＳＲＬ３０８に基づいて要求された時点で、その検証を行う必要がある。

【００９５】

ユーザがＳＲＬ３０８を自己公表すると、ユーザは、その自己公表されたＳＲＬ３０８と、そのコンテンツと同じものを生成するために使用されたＤＲＭ証明書８１０とを連結し、ＳＲＬ３０８とＤＲＭ証明書８１０付きのコンテンツは、別のユーザに配信される。そ

の後、別ユーザは、コンテンツのライセンスを、図７と図８に示す同じ方法で、ＤＲＭサーバ３２０に要求し、取得する。ここでは、ライセンスを要求するユーザは、自己公表されたＳＲＬ３０８とコンテンツに連結されたＤＲＭ証明書８１０の両方を、ＤＲＭサーバ３２０に提出する。ＤＲＭサーバ３２０は、ＤＲＭ証明書８１０の中のＳ（ＰＲ－ＤＲＭ）を、対応する（ＰＵ－ＤＲＭ）に基づいて検証し、ＤＲＭ証明書８１０から（ＰＵ－ＣＥＲＴ）を取得する。次に、ＤＲＭサーバ３２０は、ＳＲＬ３０８の中のＳ（ＰＲ－ＣＥＲＴ）を、取得した（ＰＵ－ＣＥＲＴ）に基づいて検証し、上述したように続ける。当然に理解されるように、ユーザは、ＤＲＭサーバ３２０がＳＲＬ３０８の中の権利を実施できることを検証できないので、上述したように、ＤＲＭサーバ３２０自身が、その時点で検証を行う必要がある。

【００９６】

（権利テンプレート）

上述したように、ユーザまたはユーザクラスを定義し、定義されたユーザまたはユーザクラスの各々に権利を定義し、使用条件を定義することにより、ほとんどの、どのような種類の権利データでも権利ラベルの中に生成する自由度が、ユーザに与えられている。しかし、重要なことは、特に、同じユーザまたはユーザクラス、権利および条件が、コンテンツの異なる部分ごとに繰り返し定義されるとき、複数の権利ラベルの権利データを繰り返し定義することは、煩わしく、反復的になる。このようなことは、例えば、企業やオフィス環境で起こっており、ここでは、ユーザは、定義された特定のユーザチームと共有される、コンテンツの異なる部分を繰り返し公表する。このような状況で、本発明の一実施形態では、権利テンプレートが作成され、ユーザは、権利ラベルを作成することに関して繰り返し使用することができ、ここでは、権利テンプレートは、事前に定義されたユーザまたはユーザクラス、事前に定義された各ユーザまたはユーザクラスの権利、および事前に定義された使用条件を含む。

【００９７】

本発明の一実施形態では、図１１に示すように、権利テンプレート９００は、権利ラベルの中の権利データと実質的に同じである。しかし、（ＤＥＳ１）は、コンテンツが公表されるまでは分からないので、権利データを、権利ラベルの場合と同じように、その（ＤＥＳ１）に従って暗号化することはできない。本発明の一実施形態では、暗号化されていない権利データを有する権利テンプレートを、図４のステップ４１６において（ＤＥＳ１）で権利データを暗号化する過程において提出し、（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を生成する。もちろん、権利データは、暗号化される前に、提出された権利テンプレート９００から取り出される。

【００９８】

ＤＲＭサーバ３２０とその公開鍵（ＰＵ－ＤＲＭ）は、権利テンプレートが構成される時に分かっている場合と、分かっていない場合とがある。さらに、分かっている場合でも、各々が独自の（ＰＵ－ＤＲＭ）を有するＤＲＭサーバ３２０が２つ以上存在する場合と、存在しない場合とがある。それにもかかわらず、ＤＲＭサーバ３２０とその公開鍵（ＰＵ－ＤＲＭ）が権利テンプレートの構築時に分かっている場合や、１つのＤＲＭサーバ３２０だけが採用されているか、または権利テンプレート９００に関連して１つのＤＲＭサーバだけが採用されるような場合には、権利テンプレートは、権利テンプレート９００から得られる権利ラベルに署名しようとするＤＲＭサーバに関する情報であって、公開鍵（ＰＵ－ＤＲＭ）を含む情報を含むことができる。この（ＰＵ－ＤＲＭ）は、（ＤＥＳ１）を暗号化し、その結果として（ＰＵ－ＤＲＭ（ＤＥＳ１））を得るものとして、ＳＲＬ３０８に入っているが、当然に理解されるように、（ＤＥＳ１）は、コンテンツが公表されるまで分かっていないので、権利テンプレート９００の中の（ＰＵ－ＤＲＭ）は、権利ラベルの場合と同じように、その（ＤＥＳ１）を暗号化することができない。本発明の一実施形態では、暗号化されていない（ＰＵ－ＤＲＭ）を有する権利テンプレートを、図４のステップ４１４において（ＰＵ－ＤＲＭ）で（ＤＥＳ１）を暗号化している過程で提出し、（ＰＵ－ＤＲＭ（ＤＥＳ１））を生成する。もちろん、（ＰＵ－ＤＲＭ）は、使用される

前に、提出された権利テンプレート９００から取り出される。
【００９９】
また、上述のケースでは、権利テンプレートに含むことができるＤＲＭサーバに関する他の情報は、ネットワーク上のＤＲＭサーバを探し出すためのＵＲＬなどの照会情報、およびＵＲＬが失敗したときのフォールバック情報を含むことができる。どの場合にも、権利テンプレートは、権利テンプレート９００自体を記述した情報を含むことができる。なお、権利テンプレート９００は、コンテンツおよび／または暗号化鍵（ＣＫ）と（ＤＥＳ１）とに関する権利ラベルに記述される情報などの、公表されるコンテンツに関する情報が入るスペースを提供することもできるが、権利テンプレートをインスタンス化したものが、実際には権利ラベルに変換されるのでなければ、そのスペースは不要である。
【０１００】
これまでに説明してきた権利テンプレートは、主にユーザの便宜のためのであるが、当然に理解されるように、事情によっては、ユーザが、権利ラベルに権利データを定義する自由度を制限すべきであり、権利テンプレート９００を使用して、生成される権利ラベルの範囲または種類を制限することができる。例えば、特に企業またはオフィス環境の場合には、特定のユーザが、常にコンテンツを特定のユーザクラスにのみ公表すべきこと、またはユーザが、コンテンツを特定のユーザクラスに公表してならないポリシとして、事前に定義しておくことができる。いずれの場合も、本発明の一実施形態では、このようなポリシを、事前定義された権利データとして１または複数の権利テンプレート９００に具現化し、ユーザが、コンテンツを公表するとき、その権利テンプレートを使用して権利ラベルを生成するのを制限することができる。特に、権利テンプレートまたは権利テンプレート群は、ユーザが、本発明の精神と範囲から逸脱しない限り、あらゆる種類の公表ポリシを指定することができるように、ユーザが公表ポリシを利用可能にする。
【０１０１】
制限されたユーザなどの権利テンプレート９００を指定するために、図１２を参照して説明すると、アドミニストレータなどは、実際には、事前定義された権利データを定義し（ステップ１００１）、特定のＤＲＭサーバ３２０に関する情報などの、必要で、かつ適当な他の情報を定義する（ステップ１００３）ことにより、権利テンプレート９００を構築する。重要なことは、限定されたユーザなどによって使用される権利テンプレートをもたらすためには、権利テンプレート９００を公的にしなければならない。すなわち、権利テンプレート９００は、限定ユーザなどが採用できる権利テンプレートとして認識しなければならない。従って、本発明の一実施形態では、アドミニストレータなどによって構築された権利テンプレートは、ＤＲＭサーバ３２０に提出され、これにより署名され、この署名は、権利テンプレートを公的なものにする（ステップ１００５）。
【０１０２】
署名するＤＲＭサーバ３２０は、その情報が実際に権利テンプレート９００に存在するとき、その情報が権利テンプレート９００にあるＤＲＭサーバ３２０のことである。また、ＤＲＭサーバ３２０は、必要なチェックを行ったときだけ権利テンプレート９００に署名することができ、まったくチェックなしで署名することもできる。さらに、ＤＲＭサーバからのテンプレート署名Ｓ（ＰＲ－ＤＲＭ－Ｔ）（ただし、－Ｔは、署名がＯＲＴ９００に対するものであることを意味している）は、少なくとも権利テンプレート９００の事前定義された権利データに基づくべきであるが、本発明の精神と範囲から逸脱しない限り、他の情報に基づくこともできる。以下で説明するように、署名Ｓ（ＰＲ－ＤＲＭ－Ｔ）は、権利ラベルの中に組み込まれ、権利ラベルに関連して検証され、従って、署名が基づくものがあれば、変更されない形で権利ラベルの中に組み込まれるべきである。
【０１０３】
ＤＲＭサーバ３２０が権利テンプレート９００に署名し、それをアドミニストレータなどに戻すと、アドミニストレータは、署名され、いまは公的になっている権利テンプレート９００をＳ（ＰＲ－ＤＲＭ－Ｔ）とともに受け取り（ステップ１００７）、公的権利テンプレート（ＯＲＴ）９００を１または複数のユーザに転送し、そのユーザによって使用さ

れる（ステップ１００９）。従って、ユーザがＯＲＴ９００に基づいてコンテンツを公表するために、ユーザは、ＯＲＴ９００を取り出し（ステップ１０１１）、あらゆる必要とされる情報を用意することによって、ＯＲＴ９００に基づいて権利ラベルを構築する（ステップ１０１３）。必要とされる情報は、コンテンツに関する情報、適当な鍵情報、（ＤＥＳ１）によってＯＲＴ９００から暗号化されると、結果として（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））となる権利データ、およびＯＲＴ９００からの他の情報などである。重要なことは、ユーザは、ＯＲＴ９００からの署名Ｓ（ＰＲ－ＤＲＭ－Ｔ）を権利ラベルに含む。

【０１０４】

そのあと、上述したように、ユーザは、署名のために権利ラベルをＤＲＭサーバ３２０に提出する（ステップ１０１５）。なお、ここでは、ＤＲＭサーバ３２０は、その中のＳ（ＰＲ－ＤＲＭ－Ｔ）が検証されなければ、提出された権利ラベルに署名しない。すなわち、ＤＲＭサーバ３２０は、提出された権利ラベルが、ＯＲＴ９００からの署名Ｓ（ＰＲ－ＤＲＭ－Ｔ）を含まなければ、提出された権利ラベルに署名することを拒否することにより、ユーザが、提出された権利ラベルをＯＲＴ９００に基づくべきことを強制する。具体的には、ＤＲＭサーバ３２０は、そのＳ（ＰＲ－ＤＲＭ－Ｔ）と、その署名が基づいている情報があれば、提出された権利ラベルから取り出し、（ＰＵ－ＤＲＭ）に基づいてその署名を検証する。提出された権利ラベルの権利データは、（ＤＥＳ１）に従って暗号化されている（すなわち、ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））。従って、ＤＲＭサーバ３２０は、図９を参照して上述したように、最初に（ＤＥＳ１）を取得し、それを使用して（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））を解読し、提出された権利ラベルの権利データに基づいて署名を検証することができる。

【０１０５】

検証されると、ＤＲＭサーバ３２０は、上述したように、Ｓ（ＰＲ－ＤＲＭ－Ｌ）を使用して、提出された権利ラベルに署名し、ＳＲＬ３０８を生成する（ただし、－Ｌは、署名がＳＲＬ３０８に対するものであることを意味している）。ここで、Ｓ（ＰＲ－ＤＲＭ－Ｌ）は、Ｓ（ＰＲ－ＤＲＭ－Ｔ）を置き換えることも、Ｓ（ＰＲ－ＤＲＭ－Ｔ）に付加されることもある。付加されるときは、Ｓ（ＰＲ－ＤＲＭ－Ｌ）は、Ｓ（ＰＲ－ＤＲＭ－Ｔ）の一部に基づくことができる。（ＰＲ－ＤＲＭ）は、Ｓ（ＰＲ－ＤＲＭ－Ｔ）とＳ（ＰＲ－ＤＲＭ－Ｌ）の両方を得るために使用することができるが、異なる（ＰＲ－ＤＲＭ）を、Ｓ（ＰＲ－ＤＲＭ－Ｔ）とＳ（ＰＲ－ＤＲＭ－Ｌ）の各々に使用することもできる。ＤＲＭサーバ３２０が権利ラベルに署名し、ＳＲＬ３０６８をユーザに戻すと、ユーザは、Ｓ（ＰＲ－ＤＲＭ－Ｌ）とともにＳＲＬ３０８を受け取り（ステップ１０１７）、上述したように、そのＳＲＬ３０８を公表しようとするコンテンツと連結する処理に進む。

【０１０６】

ＯＲＴ９００の署名Ｓ（ＰＲ－ＤＲＭ－Ｔ）が、少なくともＯＲＴ９００の事前定義された権利データの一部に基づいている場合には、ＳＲＬ３０８に（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ）に）入っている権利データは修正することも、変更することもできない。そうでなければ、Ｓ（ＰＲ－ＤＲＭ－Ｔ）は検証されない。それにもかかわらず、本発明の一実施形態では、ＯＲＴ９００の中の権利データは、ＯＲＴ９００に含まれる規定されたルール内で変更することができる。例えば、ルールは、２つの権利データセットの１つを、ＳＲＬ３０８に含めることを指定し、または別のセットの中から選択を可能にすることもできる。当然に理解されるように、ルールは、本発明の精神と範囲から逸脱しない限り、適当なシンタックスで記述された、どのようなルールにすることもできる。ここでは、ルールは、権利ラベルの作成時に、ユーザの適当なルールインタプリータによって解釈される。権利データは、変化することがあるが、ルールは同じように変化しないので、ＯＲＴ９００のテンプレートの署名Ｓ（ＰＲ－ＤＲＭ－Ｔ）は、権利データ自体にではなく、少なくともルールの一部に基づいている。その結果、ＯＲＴ９００に含まれるルールは、ＳＲＬ３０８に含まれていなければならない。

【０１０７】

本発明の一実施形態では、ＯＲＴ９００の事前定義された権利データは、上述したように、一部が固定で、不変であり、一部が可変で、ルール駆動（ｒｕｌｅ－ｄｒｉｖｅｎ）になっている。ここでは、ＯＲＴ９００のテンプレート署名Ｓ（ＰＲ－ＤＲＭ－Ｔ）は、少なくともルールの固定部分の一部に基づき、権利データの可変部分のルールに基づいている。

【０１０８】

当然に理解されるように、ユーザが所有しているＯＲＴ９００は、時代遅れになるか、あるいは陳腐化することがある。すなわち、権利データを通してＯＲＴ９００は、最新でなくなり、無関係となり、あるいは単純に適用できなくなったポリシを反映していることがある。例えば、ＯＲＴ９００の権利データの中で指定されている１または複数のユーザまたはユーザクラスは、ポリシ環境内に最早存在していないこともあれば、ＯＲＴ９００の権利データの中で指定された特定のユーザまたはユーザクラスは、ポリシ環境内で最早同じ権利を有していないこともある。そのようなケースでは、アドミニストレータが、改訂されたＯＲＴ９００を発行したが、ユーザは、旧版で、時代遅れのＯＲＴ９００をまだ使用していることがある。

【０１０９】

このような状況で、本発明の一実施形態では、ＤＲＭサーバ３２０が、提出された権利テンプレート９００に署名してＯＲＴ９００を生成し、ＯＲＴ９００のコピーを保存しておくと、各ＯＲＴ９００は、ユニークな識別インデックスが付けられ、ＯＲＴ９００に基づいて構築された各権利ラベルは、そのＯＲＴ９００の識別インデックスを含む。従って、図１２に示すように、提出された権利ラベルを受け取ると、ＤＲＭサーバ３２０は、権利ラベルの中からＯＲＴ９００の識別インデックスを見つけ、見つかった識別インデックスに基づいてＯＲＴ９００の最新コピーを取り出し、提出された権利ラベルから権利データを削除し、取り出したＯＲＴ９００から権利データを挿入し、最後に、少なくとも挿入された権利データの一部に基づいた権利ラベルに署名する。もちろん、ＤＲＭサーバは、（ＤＥＳ１（ｒｉｇｈｔＳｄａｔａ））を解読し、再暗号化することを含み、上述したプロセスの中で必要とされ、義務付けられと暗号化と平文化ステップを実行する。ＤＲＭサーバが、提出された権利ラベルの権利データを置換するように構成されているときには、その権利ラベルと、その権利ラベルが構築される基となったＯＲＴ９００とは、必ずしも、権利データを含む必要はない。その代わりに、権利データは、ＤＲＭサーバ３２０に置いておく必要がある。しかし、権利データを権利ラベルおよびその権利ラベルが構築される基となったＯＲＴ９００に含めることは、ユーザにとっては好都合であり、事情によっては有用なことがある。

【０１１０】

（結論）

本発明に関連して実行されるプロセスを実現するために必要なプログラミングは相対的に単純明快であり、プログラミング関係者には自明のはずである。従って、このようなプログラミングは、本明細書には添付していない。そこで、本発明の精神と範囲を逸脱しない限り、どのようなプログラミングを採用しても、本発明を実現することが可能である。

【０１１１】

以上、デジタルコンテンツとサービスに対する使用ライセンスを、署名付き権利ラベルを通して発行するためのシステムと方法を説明してきた。当業者ならば理解されるように、本発明の好適実施形態は、様々な態様に変更し、改良することが可能であり、かかる変更と改良は本発明の範囲から逸脱しない形で行うことができる。従って、請求項に記載されている本発明の範囲には、かかる等価的な変形のすべてが含まれる。

【０１１２】

付録１

【０１１３】

【表３】

権利データの例

```
<?xml version="1.0" ?>
<XrML version="1.2">
   <BODY type="Rights Template">
      <DESCRIPTOR>
         <OBJECT>
            <ID type="GUID">c43...</ID>
            <NAME>$$411$411name$411desc</NAME>
         </OBJECT>
      </DESCRIPTOR>
      <WORK>
         <OBJECT>
            <ID />
         </OBJECT>
         <RIGHTSGROUP name="MAIN RIGHTS">
            <RIGHTSLIST>
               <VIEW>
                  <CONDITIONLIST>
                     <ACCESS>
                        <PRINCIPAL>
                           <OBJECT>
                              <ID />
                              <NAME>test@company.com</NAME>
                           </OBJECT>
                        </PRINCIPAL>
                     </ACCESS>
                  </CONDITIONLIST>
               </VIEW>
               <RIGHT name="generic">
                  <CONDITIONLIST>
                     <ACCESS>
                        <PRINCIPAL>
                           <OBJECT>
                              <ID />
                              <NAME>test@company.com</NAME>
                           </OBJECT>
                        </PRINCIPAL>
                     </ACCESS>
                  </CONDITIONLIST>
               </RIGHT>
            </RIGHTSLIST>
         </RIGHTSGROUP>
      </WORK>
   </BODY>
```

【０１１４】
【表４】

```
    <SIGNATURE>
        <ALGORITHM>RSA PKCS#1-V1.5</ALGORITHM>
        <DIGEST>
            <ALGORITHM>SHA1</ALGORITHM>
            <PARAMETER name="codingtype">
                <VALUE encoding="string">surface-coding</VALUE>
            </PARAMETER>
            <VALUE encoding="base64" size="160">MwI...=</VALUE>
        </DIGEST>
        <VALUE encoding="base64" size="1024">Msi...=</VALUE>
    </SIGNATURE>
</XrML>
```

【０１１５】

付録２

【０１１６】

【表５】

署名付き権利ラベル３０８の例

```
<?xml version="1.0" ?>
<XrML version="1.2">
   <BODY type="Rights Label" version="3.0">
      <ISSUEDTIME>2002-01-01_12:00:00</ISSUEDTIME>
      <DESCRIPTOR>
         <OBJECT>
            <ID />
            <NAME>$$409$...</NAME>
         </OBJECT>
      </DESCRIPTOR>
      <ISSUER>
         <OBJECT type="DRM-Server">
            <ID type="GUID">{d81...}</ID>
            <NAME>Test DRM Server</NAME>
            <ADDRESS type="URL">http://licensing.dev.com</ADDRESS>
         </OBJECT>
         <PUBLICKEY>
            <ALGORITHM>RSA</ALGORITHM>
            <PARAMETER name="public-exponent">
               <VALUE encoding="integer32">65537</VALUE>
            </PARAMETER>
            <PARAMETER name="modulus">
               <VALUE encoding="base64" size="1024">NcO...=</VALUE>
            </PARAMETER>
         </PUBLICKEY>
         <ENABLINGBITS type="sealed-key">
            <VALUE encoding="base64" size="1024">tFg...=</VALUE>
         </ENABLINGBITS>
         <SECURITYLEVEL name="Server-Version" value="2.0" />
         <SECURITYLEVEL name="Server-SKU" value="22222-3333" />
      </ISSUER>
      <DISTRIBUTIONPOINT>
         <OBJECT type="LICENSE ACQUISITION URL">
            <ID type="GUID">{0F4...}</ID>
            <NAME>DRM Server Cluster</NAME>
            <ADDRESS type="URL">http://localhost/Licensing</ADDRESS>
         </OBJECT>
         </DISTRIBUTIONPOINT>
         <WORK>
            <OBJECT type="TEST-FORMAT">
               <ID type="MYID">FDB-1</ID>
            </OBJECT>
         <METADATA>
            <SKU type="PIDTYPE">PID</SKU>
```

【０１１７】
【表６】

```
            </METADATA>
            <PRECONDITIONLIST>
                <TIME />
            </PRECONDITIONLIST>
        </WORK>
        <AUTHDATA name="Encrypted Rights data">PAB... </AUTHDATA>
    </BODY>
    <SIGNATURE>
        <ALGORITHM>RSA PKCS#1-V1.5</ALGORITHM>
        <DIGEST>
            <ALGORITHM>SHA1</ALGORITHM>
            <PARAMETER name="codingtype">
                <VALUE encoding="string">surface-coding</VALUE>
            </PARAMETER>
            <VALUE encoding="base64" size="160">Prc...=</VALUE>
        </DIGEST>
        <VALUE encoding="base64" size="1024">EHd...=</VALUE>
    </SIGNATURE>
</XrML>
```

【図面の簡単な説明】

【図１】本発明を実現することができ、この環境に限定されない例示コンピューティング環境を示すブロック図である。

【図２】本発明を実現することができる、種々のコンピューティングデバイスが置かれている例示ネットワーク環境を示すブロック図である。

【図３】デジタルコンテンツを公表するための本発明にかかるシステムと方法の好適実施形態を示す機能ブロック図である。

【図４】権利管理されたデジタルコンテンツを公表するための本発明にかかる方法の好適実施形態を示すフローチャートである。

【図５】図４の方法によって作成された署名付き権利ラベルの構造を示すブロック図である。

【図６】権利管理されたデジタルコンテンツをライセンスするための本発明にかかるシステムと方法の好適実施形態を示す機能ブロック図である。

【図７】権利管理されたデジタルコンテンツをライセンスするための本発明にかかる方法の好適実施形態を示すフローチャートである。

【図８】権利管理されたデジタルコンテンツをライセンスするための本発明にかかる方法の好適実施形態を示すフローチャートである。

【図９】本発明の一実施形態に従って権利ラベルを再公表するとき実行される主要ステップを示すフローチャートである。

【図１０】ユーザが本発明の一実施形態に従ってオフラインの公表の実行を可能にするためにＤＲＭサーバによりユーザに発行される証明書を示すブロック図である。

【図１１】本発明の一実施形態にしたがって権利ラベルに組み込まれる情報を指定している権利テンプレートを示すブロック図である。

【図１２】本発明の一実施形態に従って図１１の権利テンプレートを生成し、権利テンプレートに基づいて図５の署名付き権利ラベルを生成するときに実行される主要ステップを示すフローチャートである。

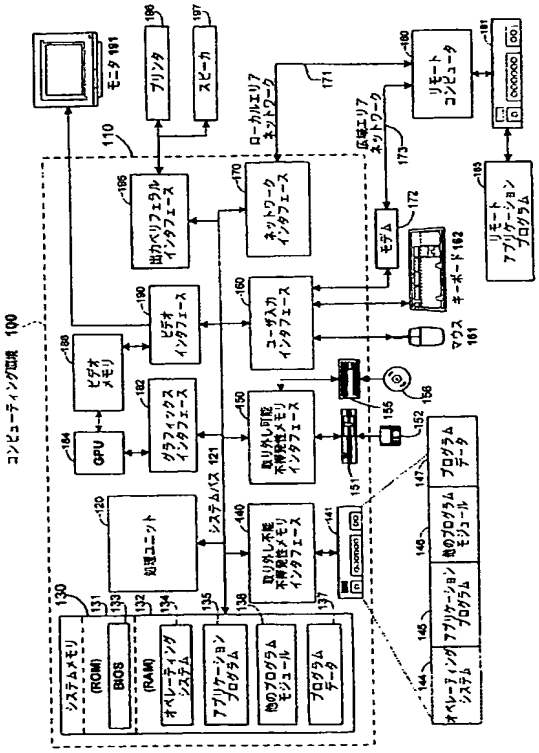
【図１３】トラストベースシステムの例の実施アーキテクチャを示すブロック図である。

【符号の説明】

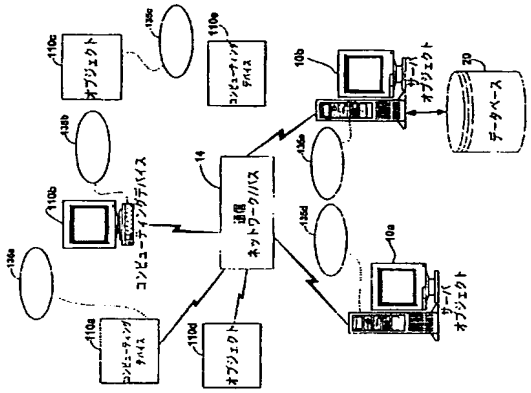
３００　クライアントデバイス

３０２　コンテンツ準備アプリケーション
３０４　暗号化デジタルコンテンツファイル
３０６　ＤＲＭクライアントＡＰＩ
３０８　署名付き権利ラベル（ＳＲＬ）
３１０　権利管理デジタルコンテンツファイル
３２０　ＤＲＭサーバ
３３０　通信ネットワーク

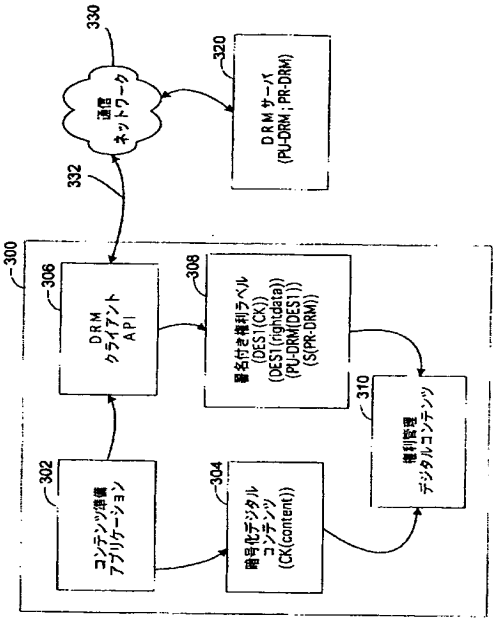
【図１】



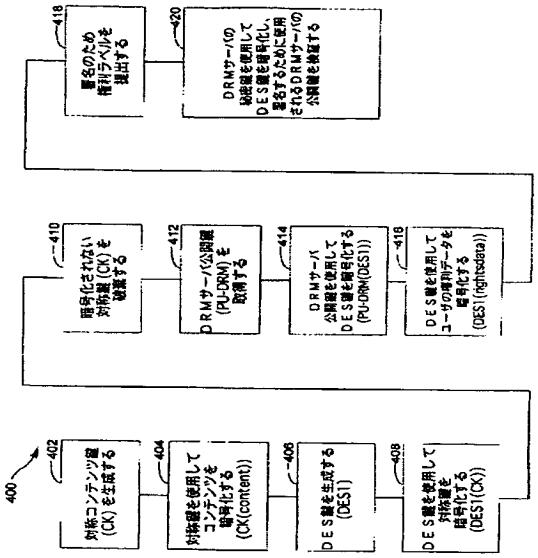
【図２】



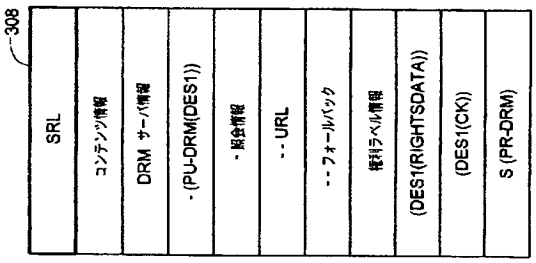
【図３】


330
通信ネットワーク
320
DRMサーバ
(PU-DRM；PR-DRM)
332
300
306
DRM
クライアント
API
308
署名付き権利ラベル
(DES1(CK))
(DES1(rightsdata))
(PU-DRM(DES1))
(S(PR-DRM))
310
権利管理
デジタルコンテンツ
302
コンテンツ準備
アプリケーション
304
暗号化デジタル
コンテンツ
(CK(content))

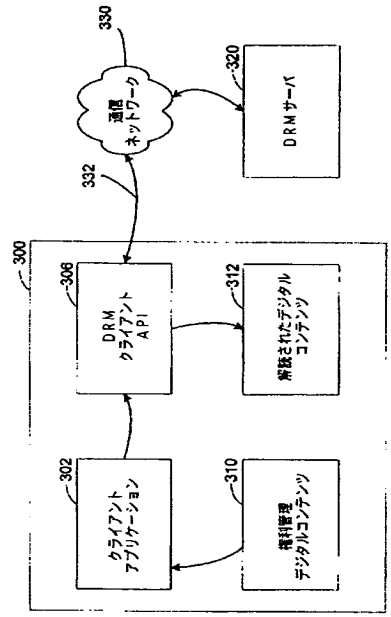
【図４】


400
402
対称コンテンツ鍵
(CK)を生成する
404
対称鍵を使用して
コンテンツを
暗号化する
(CK(content))
406
DES鍵を生成する
(DES1)
408
DES鍵を使用して
対称鍵を
暗号化する
(DES1(CK))
410
暗号化されない
対称鍵(CK)を
破棄する
412
DRMサーバ(公開鍵
(PU-DRM))を
取得する
414
DRMサーバ
公開鍵を使用して
DES鍵を暗号化する
(PU-DRM(DES1))
416
DES鍵を使用して
ユーザの権利データを
暗号化する
(DES1(rightsdata))
418
署名のため
権利ラベルを
提出する
420
DRMサーバの
秘密鍵を使用して
DES鍵を暗号化し、
署名するために使用
されるDRMサーバの
公開鍵を検証する

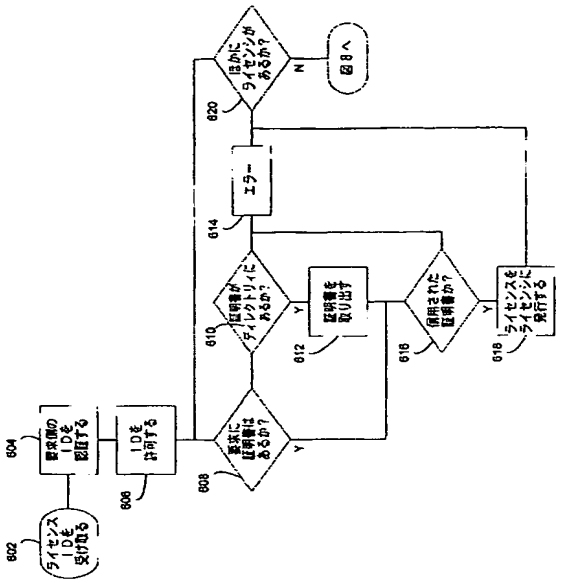
【図５】


308
SRL
コンテンツ情報
DRM サーバ情報
- (PU-DRM(DES1))
- 報酬情報
- - URL
- - フォールバック
権利ラベル情報
(DES1(RIGHTSDATA))
(DES1(CK))
S (PR-DRM)

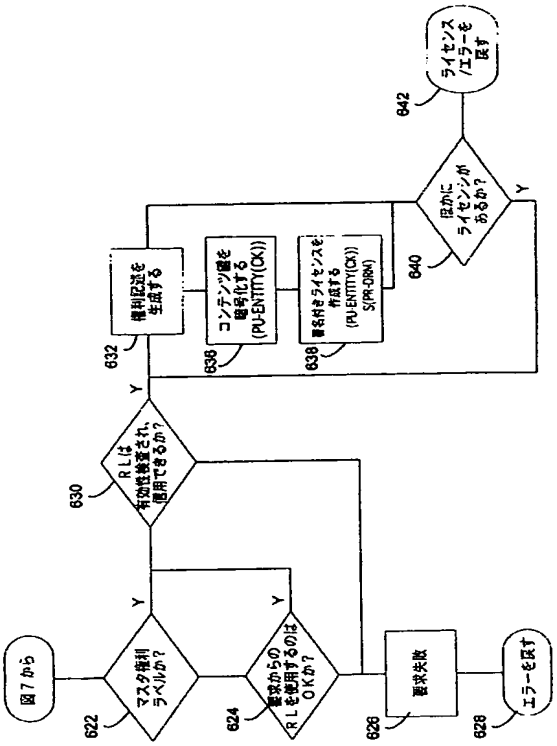
【図６】


330
通信ネットワーク
320
DRMサーバ
332
300
306
DRM
クライアント
API
312
保護されたデジタル
コンテンツ
302
クライアント
アプリケーション
310
権利管理
デジタルコンテンツ

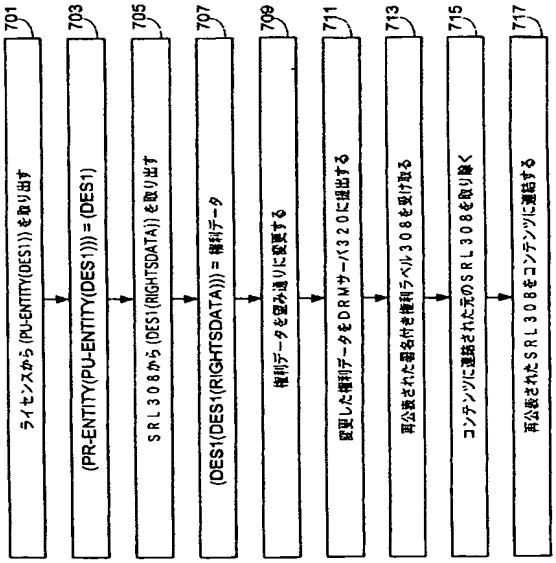
【図７】



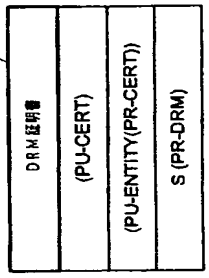
【図８】



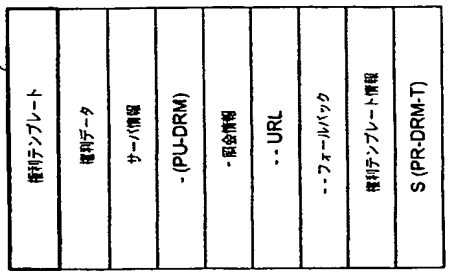
【図９】



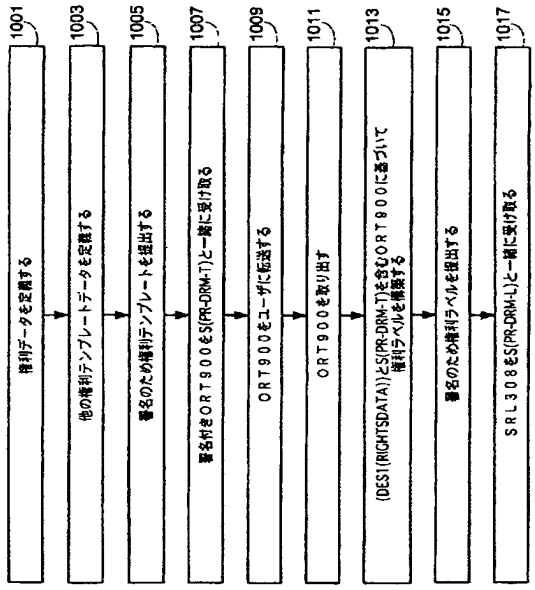
【図１０】



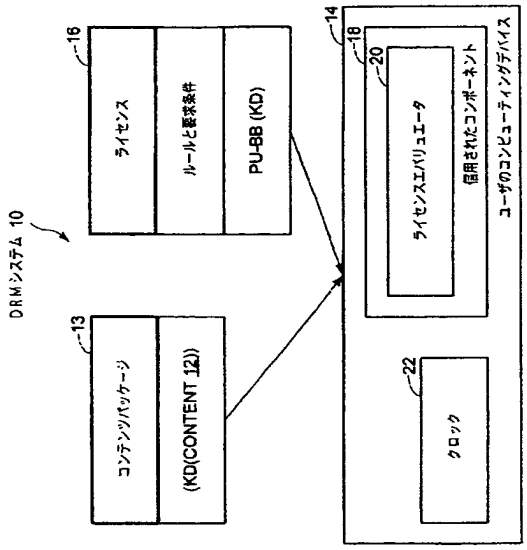
【図１１】



【図１２】


1001
権利データを定義する
1003
他の権利テンプレートデータを定義する
1005
署名のため権利テンプレートを抽出する
1007
署名付きORT900をS(PR-DRM-T)と一緒に受け取る
1009
ORT900をユーザに転送する
1011
ORT900を取り出す
1013
(DES{(RIGHTSDATA)}とS(PR-DRM-T)をORT900に基づいて権利ラベルを構築する
1015
署名のため権利ラベルを抽出する
1017
SRL308をS(PR-DRM-L)と一緒に受け取る

【図１３】


DRMシステム 10
16
ライセンス
ルールと要求条件
PU-BB (KD)
13
コンテンツパッケージ
(KD(CONTENT 12))
14
18
20
ライセンスエバリュエータ
信用されたコンポーネント
ユーザのコンピューティングデバイス
22
クロック

フロントページの続き

(72)発明者 バラシャント マリク
アメリカ合衆国 98052 ワシントン州 レッドモンド 156 アベニュー ノースイースト 4850 ナンバー313
(72)発明者 ビネー クリシュナスワミー
アメリカ合衆国 98072 ワシントン州 ウッディンビル ノースイースト 142 プレイス 23319
(72)発明者 ジェームズ ビー. ショープ ジュニア
アメリカ合衆国 98103 ワシントン州 シアトル イースタン アベニュー ノース 4413
(72)発明者 チャンドラモウリ ベンカテシュ
アメリカ合衆国 98074 ワシントン州 サマミッシュ 213 プレイス サウスイースト 414
(72)発明者 アチャラ ナリン
アメリカ合衆国 98011 ワシントン州 ボズエル ノースイースト 144 コート 87 41

Fターム(参考) 5B017 AA07 BA06 CA16
5J104 AA01 AA07 AA09 AA12 AA16 EA01 EA04 EA15 EA18 JA03
JA21 KA01 KA05 KA15 LA03 LA06 MA01 NA02 NA37 PA14